JULHO | 2023

ESTUDO SOBRE A COMUNIDADE DE COMPETÊNCIAS EM CIBERSEGURANÇA

RELATÓRIO

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

PRR Plano de Recuperação e Resiliência

Financiado pela União Europeia NextGenerationEU

REPÚBLICA PORTUGUESA

FICHA TÉCNICA

TÍTULO

Estudo sobre a comunidade de competências em cibersegurança
INESC TEC

AUTORIA DO ESTUDO

COORDENADOR:
João Marco Silva | joao.marco@inesctec.pt

EQUIPA:
Paula Cristina Rodrigues | paula.c.rodrigues@inesctec.pt
Pedro Miguel Moreira | pedro.m.moreira@inesctec.pt
Vítor Fonte | vitor.f.fonte@inesctec.pt
Diana Pinho

DESIGN EDITORIAL E INFOGRAFIA
Ana Fidalgo | anafidalgo.dsgn@gmail.com

ÍNDICE

Abreviaturas

AND	Agência Nacional de Distribuição
ANS	Autoridade Nacional de Segurança
CNCS	Centro Nacional de Cibersegurança
DLT	*Distributed Ledger Technologies*
DPO	*Data Protection Officer*
DRM	*Digital Rights Management*
ECCC	*European Cybersecurity Competence Centre*
EDIDP	*European Defence Industrial Development Programme*
eIDAS	*Electronic IDentification, Authentication and trust Services*
ENISA	*European Union Agency for Cybersecurity*
ENSC	Estratégia Nacional de Segurança no Ciberespaço
FCT	Fundação para a Ciência e a Tecnologia
GNS	Gabinete Nacional de Segurança
IaaS	*Infrastructure as a Service*
IC	Informação Classificada
I&D	Investigação e Desenvolvimento
RGPD	Regulamento Geral de Proteção de Dados
TIC	Tecnologias da Informação e Comunicação
WIPO	*World Intellectual Property Organization*

Sumário Executivo

O Estudo sobre a Comunidade de Competências em Cibersegurança em Portugal enquadra-se nas atividades do Observatório do Centro Nacional de Cibersegurança. Com o objetivo de informar as partes interessadas e suportar a definição de políticas públicas, este estudo apresenta um mapeamento dos conhecimentos, atividades, processos, tecnologias e investigações dinamizados por entidades com atuação nos múltiplos setores de atividade com competências em cibersegurança. Ao colocar em perspetiva a distribuição dos setores económicos de atuação da comunidade nacional com as fontes de financiamento da atividade em cibersegurança, viabiliza-se o diagnóstico sobre as tendências de desenvolvimento e necessidades de investimento nacionais.

A caracterização da comunidade nacional de competências em cibersegurança é sustentada pela identificação de entidades dos tecidos empresarial e académico com atuação na área e posterior aplicação de um inquérito *on-line* inspirado no *Cybersecurity Competence Survey*, publicado pela *European Union Agency for Cybersecurity* (ENISA). Os dados obtidos neste questionário são complementados pelo levantamento sistemático de dados de domínio público sobre a atividade comercial e científica dessas entidades e por entrevistas a interlocutores de algumas instituições selecionadas.

O resultado desta abordagem é um volume significativo de informação que permite múltiplas formas de análise e de diagnóstico dos diferentes domínios da cibersegurança por leitores de diferentes setores e com objetivos diversos. Nesse sentido e a título de exemplo, este estudo permite perceber a importância determinante de financiamentos nacionais e europeus no desenvolvimento de projetos em cibersegurança por parte das entidades nacionais participantes. Da mesma forma, permite conhecer o posicionamento do setor privado, dos centros de investigação e do ensino superior relativamente à captação destes financiamentos e como fontes de financiamento próprio. Tendo por base o número de registos de *software* e patentes, o estudo aponta ainda para o que parece ser uma menor apetência ou dificuldade das entidades nacionais em traduzirem os resultados dos projetos de investigação e inovação em produtos e serviços disponíveis no mercado. Juntam-se ainda indicadores relativos à produção científica e, de um modo geral, à atividade das entidades participantes no estudo nos diferentes domínios da cibersegurança.

O conhecimento destes e de outros indicadores, não só permite uma melhor compreensão da comunidade nacional de competências no domínio da cibersegurança, como pode e deve contribuir para a definição de futuras políticas públicas e planos de ação concretos que visem a implementação da Estratégia Nacional de Segurança no Ciberespaço (ENSC)[1]

O levantamento iniciado com este estudo, deverá ainda servir de base para, a seu tempo, não só a identificação de tendências nas suas diferentes vertentes, mas também como contribuição para aferir o impacto das futuras políticas públicas numa comunidade de competências que se pretende cada vez mais dinâmica e participante na persecução do desígnio nacional de segurança do nosso ciberespaço.

1 https://www.cncs.gov.pt/pt/estrategia-nacional/

1. Nota Metodológica

Tendo em conta a ENSC, a metodologia adotada no desenvolvimento do *Estudo sobre a Comunidade de Competências em Cibersegurança em Portugal* busca compreender e relatar de forma sistemática os conhecimentos, tecnologias, investigações e resultados produzidos em território nacional pelos diferentes setores da economia. O foco principal deste levantamento centra-se nas entidades responsáveis pelo panorama atual e pelo desenvolvimento de competências nacionais em cibersegurança.

Para isso, o estudo assume duas vertentes metodológicas principais, responsáveis por produzir indicadores capazes de (a) descrever o panorama da investigação e desenvolvimento no âmbito nacional; (b) caracterizar, quantitativamente e qualitativamente, a produção e disseminação de conhecimento promovidas pela comunidade de competências, assim como a capacidade de atração de investimento; e (c) identificar os setores económicos nos quais as competências em cibersegurança são desenvolvidas e aplicadas. Mais especificamente, as vertentes metodológicas são:

- Levantamento sistemático aplicado a fontes primárias de domínio público com o objetivo de identificar e caracterizar as entidades de diferentes setores com atividade nacional na área da cibersegurança. A caracterização das atividades, assim como a estrutura do presente relatório, seguem a proposta europeia para uma taxonomia das competências em cibersegurança[2], publicada pela *European Union Agency for Cybersecurity* (ENISA). Esta abordagem permitirá futuras análises comparativas dos resultados nacionais alcançados relativamente aos centros de competências em cibersegurança existentes no contexto europeu.
- Aplicação de um questionário on-line às entidades identificadas na primeira vertente com o objetivo de aprofundar as dimensões da caracterização da comunidade nacional de competências em cibersegurança. O questionário é inspirado no *Cybersecurity Compentence Survey*, publicado pelo *European Cybersecurity Centre of Expertise* (ECCC). Este alinhamento é fundamental para produzir indicadores que contextualizem Portugal no panorama europeu. Além disso, um conjunto de entrevistas aos intervenientes de algumas das entidades que responderam ao questionário on-line consolidam os resultados obtidos em ambas as vertentes metodológicas do estudo. A este propósito, é importante sublinhar que os períodos de observação deste estudo e do estudo no qual se baseia não são coincidentes pelo que, apesar de permitirem uma desejável contextualização do caso nacional no âmbito europeu, não é possível, no entanto, uma comparação direta entre seus indicadores.

A Tabela 1.1 apresenta os domínios de competências introduzidos pela taxonomia da ENISA e usados neste estudo para mapear as atividades em cibersegurança de entidades nacionais. Com o objetivo de evitar inconsistências oriundas do processo de tradução, a tabela apresenta também os termos originais, em inglês, dessa taxonomia. Uma lista com todos os domínios e subdomínios considerados neste estudo é apresentada no Anexo B.

TABELA 1.1: DOMÍNIOS DE COMPETÊNCIAS EM CIBERSEGURANÇA DE ACORDO COM A TAXONOMIA DA ENISA.

Identificador	Domínio em Cibersegurança
D01	Garantia, Auditoria e Certificação *Assurance, Audit and Certification*
D02	Criptologia *Cryptology*
D03	Segurança de Dados e Privacidade *Data Security and Privacy*
D04	Tratamento/Resposta de Incidentes e Ciência Forense Digital *Operational Incident Handling and Digital Forensics*
D05	Fatores Humanos *Human Factors*

2 https://op.europa.eu/s/wl2d

Identificador	Domínio em Cibersegurança
D06	Gestão de Identidade e Acesso *Identity and Access Management*
D07	Gestão e Governação de Segurança *Security Management and Governance*
D08	Rede e Sistemas Distribuídos *Network and Distributed Systems*
D09	Engenharia de Segurança de *Software* e *Hardware* *Software and Hardware Security Engineering*
D10	Medidas de Segurança *Security Measurements*
D11	Tecnologia e Aspetos Legais *Technology and Legal Aspects*
D12	Fundamentos Teóricos da Análise e de Desenho de Segurança *Theoretical Foundations of Security Analysis and Design*
D13	Gestão de Confiança, Garantia de Segurança e Rastreabilidade *Trust Management, Assurance, and Accountability*

Ainda sobre as vertentes metodológicas, na primeira fase foram identificadas 212 entidades de diferentes setores que divulgam publicamente algum tipo de atividade relacionada com a cibersegurança. A Tabela 1.2 apresenta a distribuição destas entidades por tipo principal de atividade. Detalhes sobre cada grupo de entidades são apresentados ao longo deste estudo. Contudo, é importante ressalvar que as 120 entidades empresariais correspondem ao subconjunto dos associados coletivos das associações e polos de empresas em TIC listados na Tabela 2.1 que declaram, nas respetivas páginas na Internet, fornecer produtos ou serviços nos vários domínios da cibersegurança[3].

TABELA 1.2: ENTIDADES COM ATIVIDADE EM CIBERSEGURANÇA POR TIPO PRINCIPAL DE ATIVIDADE.

Número de Entidades	Tipo de Entidade
120	Entidades empresariais de diferentes setores
8	Associações e polos de empresas em TIC
6	Organismos do Estado ou empresas públicas
28	Instituições públicas de ensino superior
17	Instituições privadas de ensino superior
21	Centros de investigação
12	Instituições de formação especializada e certificação técnica

A aplicação do questionário on-line foi antecedida por um convite institucional enviado pelo CNCS a 92 entidades. O pedido de colaboração no estudo ao tecido empresarial foi feito por intermédio das associações e polos de empresas de TIC. Deste total, 51 entidades expressaram disponibilidade em participar nesta vertente do estudo. Já o número total de entidades a fornecer respostas válidas ao questionário foi 32. Esta é uma participação mais expressiva do que a observada no estudo semelhante conduzido pela *European Cybersecurity Centre of Expertise*, i.e., *Cybersecurity Compentence Survey*, que obteve apenas resposta de 19 entidades com atividade em Portugal. Este mesmo estudo, que contou com 655 centros de competência em 36 países, é usado como referência para a avaliação comparativa entre a realidade nacional e europeia.

Os diferentes indicadores e dimensões do estudo que permitem a caracterização da comunidade nacional de competências em cibersegurança são detalhados ao longo da discussão dos resultados neste documento e correspondem às atividades desenvolvidas pelas diferentes entidades entre janeiro de 2017 e dezembro de 2021.

3 O total de associados coletivos das entidades listadas é 655.

2. CARACTERIZAÇÃO DA COMUNIDADE DE COMPETÊNCIAS

2. Caracterização da Comunidade de Competências

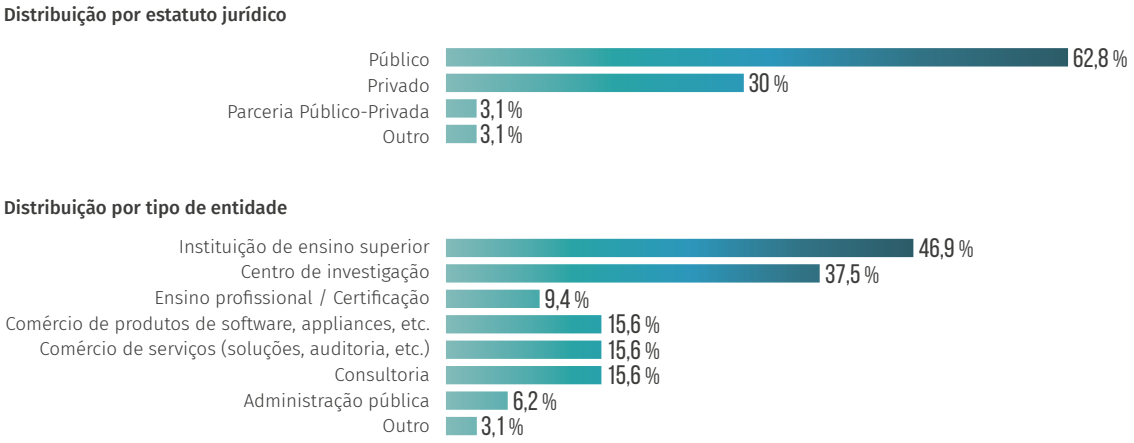
2.1. Entidades, Atividades e Fontes de Financiamento

A caracterização das comunidades de competências em cibersegurança passa, numa primeira fase, pela classificação das entidades com atividade nos diversos domínios da área em Portugal. Para isso, o estudo usa como fonte principal as respostas fornecidas ao questionário on-line, introduzido no Capítulo 1 e detalhado no Anexo A. A informação resultante é complementada por levantamentos de dados on-line de domínio público. A origem dos dados que sustentam cada dimensão desta caracterização é apresentada ao longo da discussão sobre os resultados obtidos.

Tendo em consideração o objetivo de descrever o panorama nacional na área de cibersegurança, é relevante mencionar que a maior parte das respostas ao questionário on-line são provenientes de entidades com sede administrativa em Portugal (i.e., 97% das respostas). De acordo com a Figura 2.1, há uma predominância de entidades públicas dedicadas às atividades de ensino superior e investigação científica, seguidas por entidades privadas dedicadas, maioritariamente, ao comércio de produtos e serviços, assim como consultoria. Distribuição semelhante é observada entre os 655 centros de competência europeus que participaram no estudo do ECCC.

FIGURA 2.1: ESTATUTO JURÍDICO E TIPO DE ENTIDADE

Existem entidades com atividades em mais de uma classe.



Apesar de o questionário on-line ter sido respondido por 28 instituições de ensino superior ou centros de investigação, o levantamento sobre a produção científica nacional em cibersegurança (descrita na Secção 2.2) revela que 37 instituições destes tipos demonstram atividade no setor. A significativa participação dessas instituições corrobora a relevância do retrato nacional apresentado neste estudo.

Mesmo com uma participação proporcionalmente inferior nas respostas ao questionário on-line, o levantamento feito aos diretórios das principais associações e polos de empresas do setor das Tecnologias de Informação e Comunicação revelou 122 entidades com atuação em cibersegurança. Essas empresas, de de natureza privada, dedicam-se às atividades na área da consultoria, auditoria, ensino profissional e ao comércio de produtos e serviços e correspondem a 20% do total de associados coletivos das entidades listadas na Tabela 2.1.

TABELA 2.1: ASSOCIAÇÕES E POLOS DE EMPRESAS EM TIC.

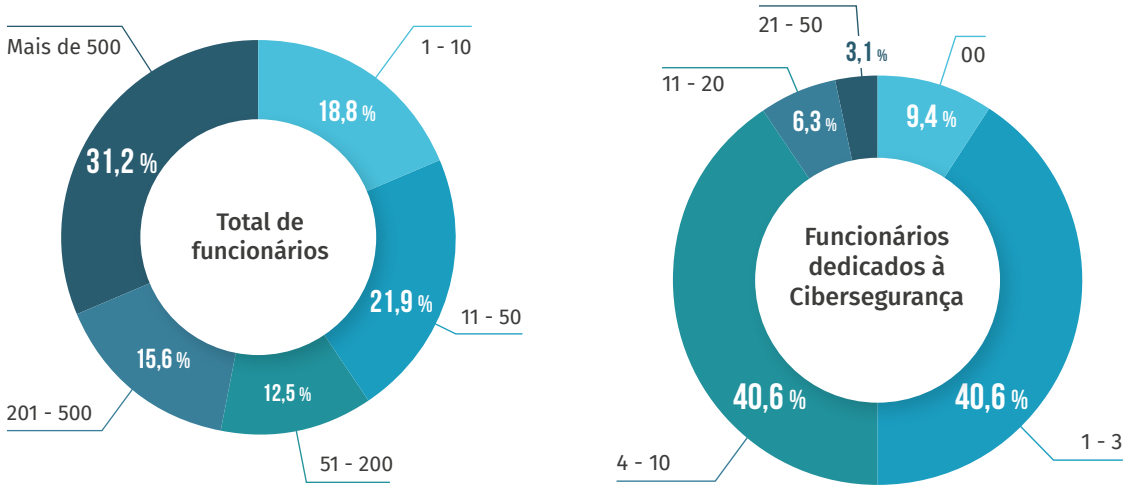
Nome da Entidade
Associação TICE.PT - Pólo das Tecnologias de Informação, Comunicação e Electrónica
ANETIE – Associação Nacional das Empresas das Tecnologias de Informação e Electrónica
APDSI - Associação para a Promoção e Desenvolvimento Sociedade da Informação
AETICE - Associação das Empresas de Tecnologias de Informação, Comunicação e Eletrónica
itSMF Portugal - Associação Portuguesa de Gestores de Serviços de Tecnologias de Informação
ASSOFT - Associação Portuguesa de *Software*
APDC - Associação Portuguesa para o Desenvolvimento das Comunicações
AP2SI - Associação Portuguesa para a Promoção da Segurança da Informação

A partir da identificação inicial das entidades empresariais com atividade em cibersegurança, a análise individual dos produtos, serviços, parcerias e tecnologias descritos nas respetivas páginas da Internet sustenta a caracterização das competências setoriais à luz da taxonomia proposta pela ENISA (ver Tabela 1.1). Tal como discutido no Capítulo 3, esta vertente exploratória do estudo complementa e ratifica os resultados obtidos através do questionário on-line, revelando a adequação da metodologia adotada.

Ao relacionar a dimensão das entidades em número total de funcionários, observa-se uma concentração de organizações de grande dimensão[4]. Além disso, as respostas evidenciam a dinâmica das instituições nacionais relacionada com a cibersegurança, uma vez que mais de 70% de todas as entidades possuem entre um e dez funcionários exclusivamente dedicados a tais atividades. Por outro lado, cerca de 9% não dispõem de especialistas dedicados nos seus quadros. Além disso, é possível observar que os resultados não demonstram uma correlação clara entre o número total de funcionários e o tamanho das equipas dedicadas à cibersegurança.

FIGURA 2.2: DIMENSÃO DAS ENTIDADES QUE RESPONDERAM AO QUESTIONÁRIO ON-LINE.

As entidades são dimensionadas pelo número total de funcionários e pelo número de funcionários dedicados à cibersegurança. Por exemplo, 31.2% das entidades possuem mais de 500 funcionários e 6.3% das entidades possuem entre 11 e 20 funcionários exclusivamente dedicados à atividade em cibersegurança.



No que diz respeito às fontes de financiamento da atividade em cibersegurança, há uma significativa relevância dos programas europeus e nacionais de inovação e investigação. Tal como representado na Figura 2.3, mais de 48% das entidades que respondeu ao questionário on-line financiam atividades especializadas através destes tipos de fontes. Proporção idêntica à observada pelo *European Cybersecurity Competence Centre* (ECCC) no estudo que analisou centros de excelência de 36 países europeus. Outro destaque é o financiamento próprio da atividade em cibersegurança, uma realidade de aproximadamente 14% das

4 O Instituto Nacional de Estatística segue uma Recomendação da Comissão Europeia de 6 de maio de 2003 que define como *Grande Empresa* aquela com número igual ou superior a 250 funcionários.

entidades consideradas. A Figura 2.4 estende esta análise e demonstra que a importância dos programas de financiamento é transversal a todos os domínios de competências em cibersegurança.

FIGURA 2.3: FONTES DE FINANCIAMENTO DA ATIVIDADE EM CIBERSEGURANÇA.

Financiamento entre 2017 e 2021 das entidades nacionais que responderam ao questionário on-line.

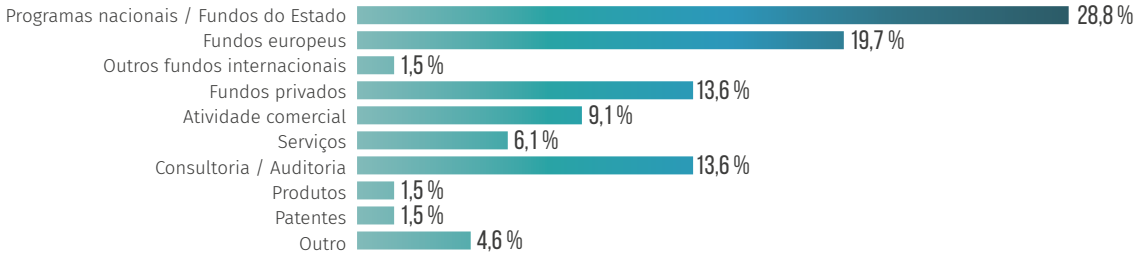
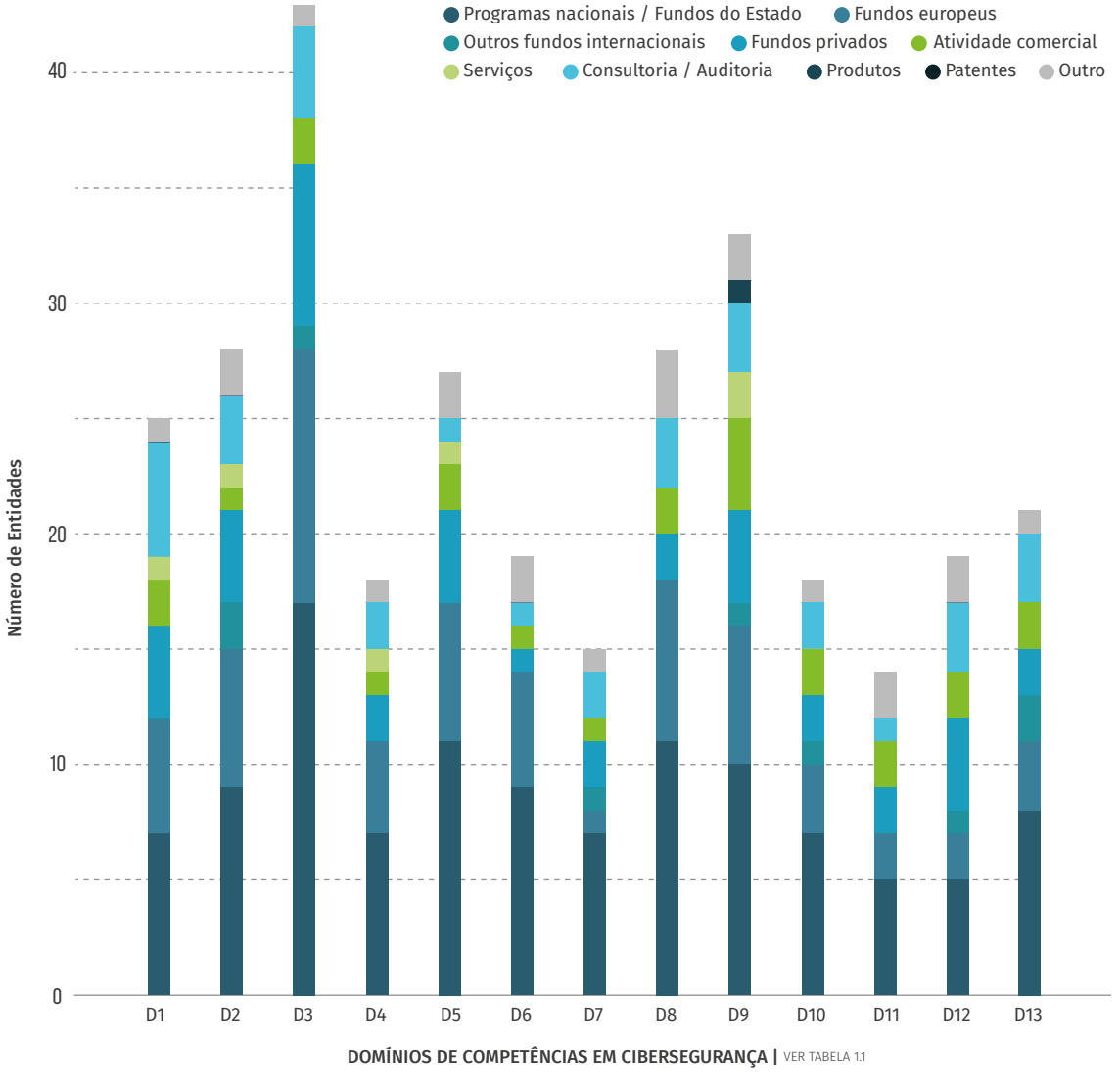


FIGURA 2.4: FONTES DE FINANCIAMENTO POR DOMÍNIOS DE COMPETÊNCIA.

Financiamento entre 2017 e 2021 das entidades nacionais que responderam ao questionário on-line



De acordo com os dados publicados pela Comissão Europeia[5], 38 entidades portuguesas estiveram envolvidas em 30 projetos financiados através de programas europeus para inovação e investigação na área de cibersegurança, no período entre 2017 e 2021. No total, o volume de financiamento captado pelas entidades nacionais ultrapassa o valor de 13.7 milhões de euros e, em oito destes projetos, aparecem como coorde-

5 https://cordis.europa.eu/

nadoras dos respetivos consórcios. Observa-se também uma participação significativa do tecido industrial, uma vez que 22 das entidades são de natureza privada, seguido por instituições de ensino superior e por centros de investigação (*i.e.,* 13 entidades). Esta predominância mantém-se quando considerados os projetos coordenados por entidades portuguesas, onde cinco são do setor privado e três do ensino superior ou centros investigação. A Tabela 2.2 lista as entidades nacionais que coordenaram projetos europeus no período considerado neste estudo.

TABELA 2.2: ENTIDADES NACIONAIS QUE COORDENARAM PROJETOS EUROPEUS NOS CINCO ANOS ANALISADOS.

Projeto	Nome da Entidade
CyberSANE	PDM & FC Projecto Desenvolvimento Manutenção Formação e Consultadoria LDA
LOQR	LOQR SA
BIECO	UNINOVA - Instituto de Desenvolvimento de Novas Tecnologias
YAKSHA	Sociedade Portuguesa de Inovação Consultadoria Empresarial e Fomento da Inovação SA
LUMIMOF	Universidade de Aveiro
FogProtect	UBIWHERE LDA
ARCADIAN-IoT	Intituto Pedro Nunes Associado para a Inovação e Desenvolvimento em Ciência e Tecnologia
IRIS	INOV - Instituto de Engenharia de Sistemas e Computadores, Inovação

No contexto dos programas nacionais de financiamento à investigação e inovação, de acordo com a Fundação para a Ciência e a Tecnologia (FCT)[6], nos últimos cinco anos, 11 projetos com temas centrais diretamente relacionados com a cibersegurança foram recomendados para financiamento em quatro editais do *Concurso de Projetos de I&D em Todos os Domínios Científicos* e do *Concurso para Projetos Exploratórios no âmbito do Programa Canegie Mellon Portugal*. Os projetos financiados foram propostos, na sua totalidade, por instituições de ensino superior ou centros de investigação e captaram um investimento aproximado de 1.6 milhões de euros. A Tabela 2.3 lista as entidades com projetos financiados via concursos nacionais. Contudo, é importante ressalvar que entrevistas a coordenadores de alguns destes projetos revelaram que há instituições privadas participantes nos consórcios não identificadas no portal da FCT.

TABELA 2.3: ENTIDADES COORDENADORAS DE PROJETOS DE FUNDOS NACIONAIS.

Nome da Entidade	
INESC TEC	Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência
IT	Instituto de Telecomunicações
FCIÊNCIAS.ID	Associação para a Investigação e Desenvolvimento de Ciências
FCUP	Faculdade de Ciências da Universidade do Porto
INESC-ID	Instituto de Engenharia de Sistemas e Computadores, Investigação e Desenvolvimento em Lisboa
NOVA-ID	Associação para a Inovação e Desenvolvimento da Faculdade de Ciência e Tecnologia da Universidade Nova de Lisboa

No que diz respeito à atividade comercial de produtos, serviços e de consultoria, destacam-se os contratos com a indústria e com governos, identificados por mais de 50% das instituições como fonte de financiamento da atividade em cibersegurança. Além disso, importa destacar a baixa proporção de financiamento oriundo da exploração de registos de *software* e de patentes. Situação semelhante à observada pelo ECCC no estudo que avaliou 655 centros europeus de competência em cibersegurança. No que diz respeito ao registo de patentes, o levantamento do *World Intellectual Property Organization* (WIPO)[7] indica que, no intervalo considerado de cinco anos, foram concedidas 13 patentes a inventores ligados a cinco instituições nacionais.

A Figura 2.5 demonstra a distribuição da atividade comercial entre as entidades participantes do estudo. De notar que, de acordo com as respostas ao questionário on-line, não existe uma relação de proporcio-

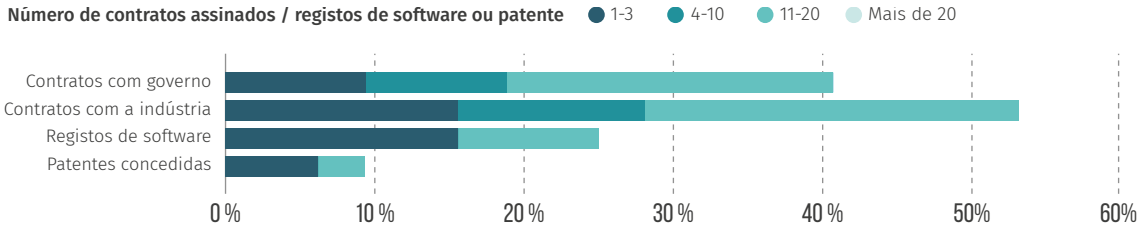
6 https://www.fct.pt/acessoaberto/index.phtml.en
7 https://www.wipo.int/

nalidade entre o número de patentes registadas e o número de funcionários dedicados à atividade de cibersegurança. Neste sentido, equipas especializadas de até três profissionais são responsáveis por cerca de 75% das patentes obtidas.

Ainda sobre os registos de patentes, de acordo com o levantamento feito no WIPO, uma única entidade do setor privado obteve cinco patentes relacionadas com métodos de processamento, gestão e acesso a dados médicos anonimizados. No total, oito patentes foram originadas de desenvolvimentos no setor privado. As instituições de ensino e centros de investigação estiveram envolvidas na obtenção de cinco das patentes relacionadas com comunicações seguras e com métodos de proteção contra falsificações. Neste último caso, três patentes são resultado de inovação liderada por uma empresa pública.

FIGURA 2.5: ATIVIDADE COMERCIAL E DE CONSULTORIA.

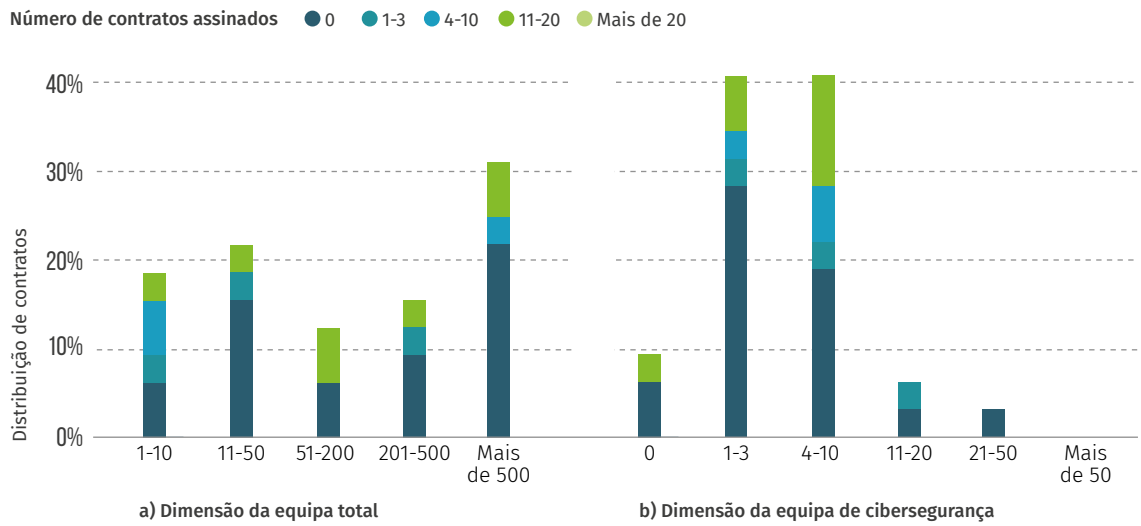
Distribuição das entidades que indicaram ter assinado contratos, obtido registos de softwares e de patentes relacionadas com cibersegurança entre 2017 e 2021. Por exemplo, cerca de 10% assinou entre 1 e 3 contratos com entidades públicas, enquanto pouco mais de 20% assinou entre 11 e 20 contratos com entidades de mesma natureza.



Cumpre notar que o desempenho das entidades em termos de contratos assinados para atividades em cibersegurança está mais diretamente relacionado com a dimensão da entidade do que com o tamanho das equipas especializadas. A Figura 2.6 apresenta os contratos com entidades de natureza pública para demonstrar esta relação.

FIGURA 2.6: RELAÇÃO ENTRE DIMENSÃO DAS EQUIPAS E OS CONTRATOS COM ENTIDADES DE NATUREZA PÚBLICA.

A distribuição considera as dimensões das equipas totais e dedicadas à cibersegurança no período entre 2017 e 2021. Por exemplo, cerca de 30% das entidades com equipas compostas por 1 a 3 funcionários dedicados à cibersegurança afirmaram não ter assinado contratos com entidades públicas no período.



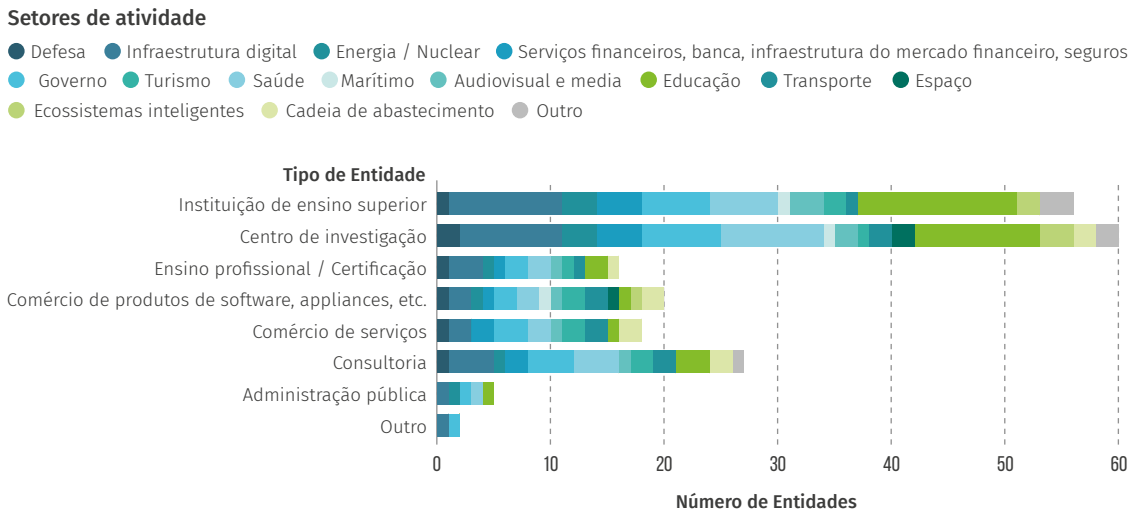
Uma vertente importante da caracterização da atividade nacional em cibersegurança é a identificação e classificação da atividade por setores da economia. A Figura 2.7 detalha os setores[8] de aplicação, relacionando-os com o tipo de entidade. Apesar de o maior número de instituições de ensino superior e de investigação a responder o questionário on-line ser refletido na alta concentração de atividade em *educação*, há um volume semelhante de atividade no setor de *infraestruturas digitais*. Os setores ligados ao *governo*, *saúde* e *transporte* também são destaques relevantes. É interessante observar que mesmo a área de *infraestruturas digitais* tem como principais atores as instituições de ensino superior e os centros de investigação. As entidades dedicadas ao comércio de produtos, como *software* e *appliances* de segurança,

8 O Anexo C detalha a dimensão setorial do estudo.

demonstram uma distribuição de atividade mais homogénea entre os diferentes setores. Curiosamente, a entidade com maior concentração de atividade no setor de *defesa* não forneceu identificação de nome ou tipo de entidade, o que salienta a sensibilidade da cibersegurança neste setor.

FIGURA 2.7: SETORES DE ATUAÇÃO POR TIPO DE ENTIDADE.

Existem entidades com atividade em cibersegurança aplicada a múltiplos setores no período entre 2017 e 2021.



Ainda sobre o setor da *educação*, entidades de ensino profissional e certificação técnica são particularmente ativas em Portugal e cobrem um conjunto de tópicos que se alinham com a procura das principais áreas de aplicações e tecnologias, nomeadamente, os *sistemas de informação* (ver Figura 2.8). A Tabela 2.4 lista os principais cursos profissionalizantes e as certificações técnicas em cibersegurança oferecidas pelas 12 maiores instituições dedicadas a esta atividade. Esta lista é resultado do levantamento efetuado a partir das respetivas páginas na Internet.

TABELA 2.4: OFERTA DE FORMAÇÃO ESPECIALIZADA E CERTIFICAÇÃO TÉCNICA.

O quadro representa o cenário nacional em junho de 2022.

Formações Especializadas
Especialização Avançada em Cibercrime e Cibersegurança
Técnico em Segurança
Auditor de Segurança
Data Protection Officer (DPO)
Segurança em *Cloud*
Fundamentos de Segurança e Informática
Information Security Management ISO/IEC 27001/27002
Security Incident Response
Técnico Especialista em Cibersegurança
Segurança de Redes
Conformidade Legal - RGPD e ISO/IEC 27001:2013
Gestão da Cibersegurança
Gestão da Privacidade
Aplicações Criptográficas para a Segurança da Informação
Segurança e Gestão da Privacidade na *Cloud*
Segurança das Comunicações
Ethical Hacking Fundamentals
Hacking Aplicações WEB
Hacking com MetaSploit

Certificações Técnicas
AWS security essentials
Certified network defender
CompTIA cybersecurity analyst
CompTIA Security+
Computer hacking forensic investigator
Ethical hacking and countermeasure
Microsoft security operations analyst
Microsoft azure security technologies
ISO/IEC 27001
ISO/IEC 20000-1 - Sistema de gestão de serviços
ISO/IEC 27701 - Gestão de informação privada

Ao comparar a distribuição da atividade por setores da economia entre as entidades portuguesas analisadas neste estudo e as entidades europeias que participaram no estudo do ECCC, é possível observar algumas convergências relevantes. Como ilustrado na Figura 2.8, os setores da Infraestrutura Digital, Governo e Saúde concentram o maior número de entidades. Por outro lado, nos setores de Defesa e de Ecossistemas inteligentes, há uma concentração ligeiramente superior no panorama agregado continental quando comparado ao nacional. É importante mencionar que, de acordo com o estudo do ECCC, os setores em que são necessários grandes investimentos em infraestrutura de investigação e desenvolvimento tendem a ser melhor explorados por países onde tradicionalmente há mais recursos disponíveis. Como ilustrado na Figura 2.8, em ambos os contextos, os setores da Infraestrutura digital, Governo e Saúde concentram o maior número de entidades. Por outro lado, os setores da Defesa e dos Ecossistemas inteligentes apresentam uma maior diferença no número de entidades no cenário nacional comparado com o cenário europeu.

Uma outra dimensão da caracterização das entidades nacionais baseia-se nas áreas de aplicações e tecnologias para as quais a atividade em cibersegurança é destinada. A Figura 2.9 apresenta o total das respostas dadas ao questionário on-line, levando em consideração todos os domínios em cibersegurança apresentados na Tabela 1.1. Tal como é possível observar, há um maior volume de atividade relacionada com os *sistemas de informação*, *sistemas operativos* e *infraestruturas críticas*. A área da *computação em nuvem e virtualização* tem vindo a ganhar atenção, na medida em que o número de serviços que adotam soluções sustentadas em infraestruturas como um serviço é cada vez maior (*i.e., Infrastructure as a Service* - IaaS). Por outro lado, apesar do rápido crescimento e do interesse global, as áreas de *sistemas veiculares* e *robótica* correspondem ao menor volume de atividade entre as entidades que responderam ao questionário on-line. Este panorama representa potenciais áreas de investimento nacional nos próximos anos.

FIGURA 2.8: DISTRIBUIÇÃO COMPARADA DOS SETORES DE ATIVIDADE - PORTUGAL E UNIÃO EUROPEIA.

Considera a atividade nacional entre 2017 e 2021 através das respostas ao inquérito on-line e a atividade europeia publicada no estudo do ECCC.

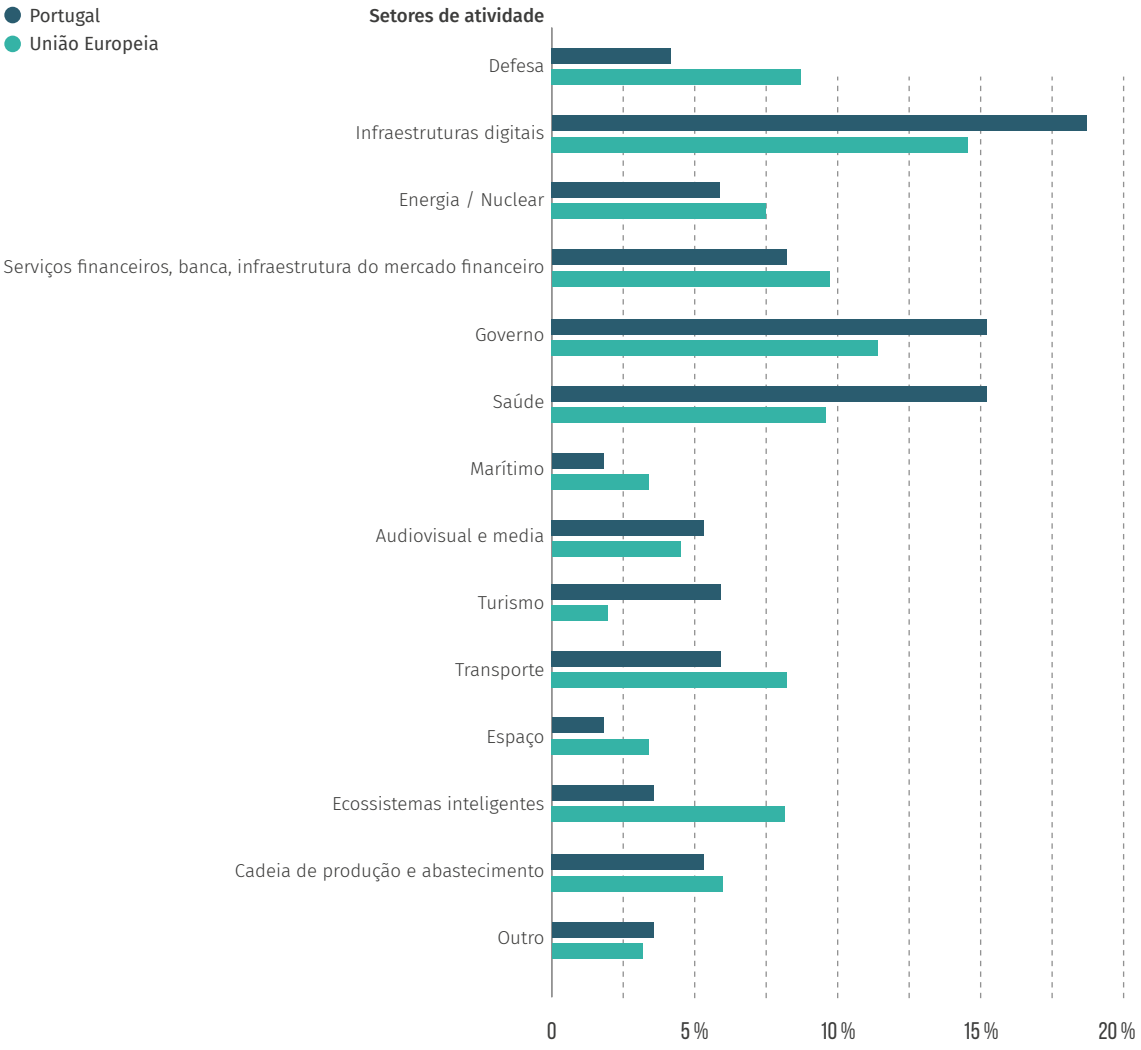
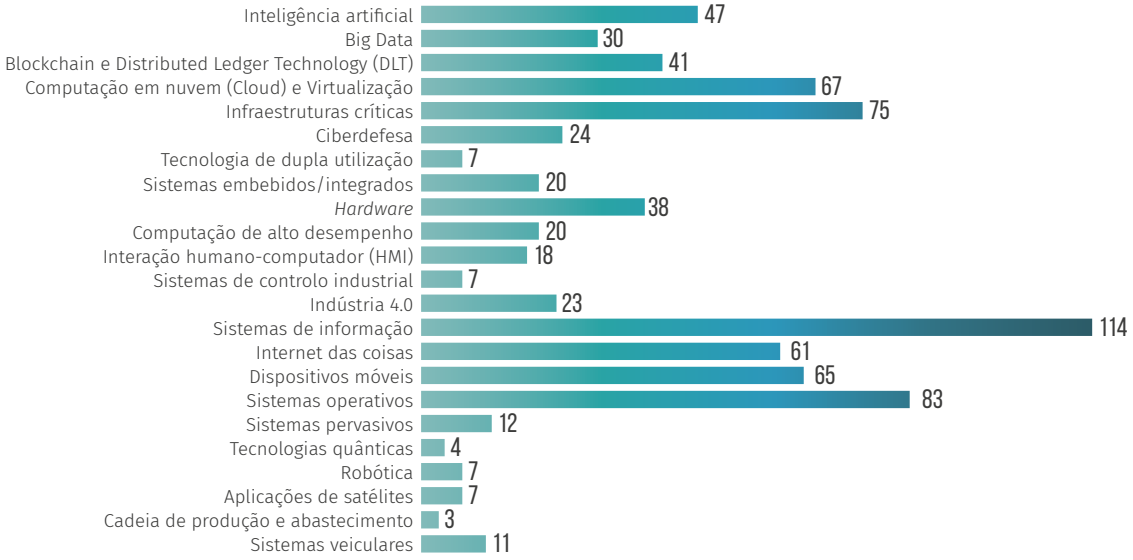


FIGURA 2.9: ÁREAS DE APLICAÇÕES E TECNOLOGIAS - PORTUGAL.

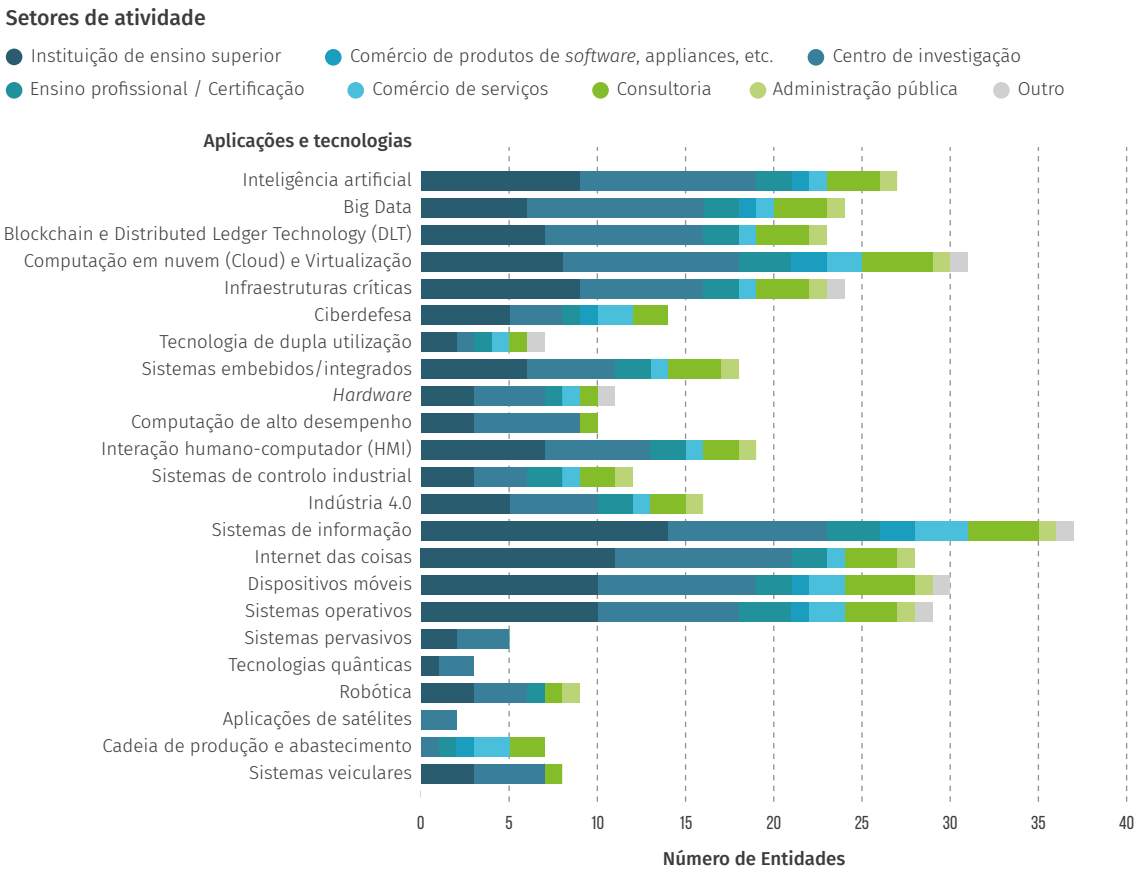
Total das respostas ao questionário on-line para a indicação das áreas de aplicação e tecnologias relacionadas com a atividade em cibersegurança considerando todos os domínios de competências.



Contrariamente à concentração observada nos setores onde a atividade em cibersegurança é aplicada por tipo de entidade, as aplicações e tecnologias demonstram uma distribuição mais homogénea (ver Figura 2.10).

FIGURA 2.10: ÁREAS DE APLICAÇÕES E TECNOLOGIAS POR SETOR DE ATIVIDADE - PORTUGAL.

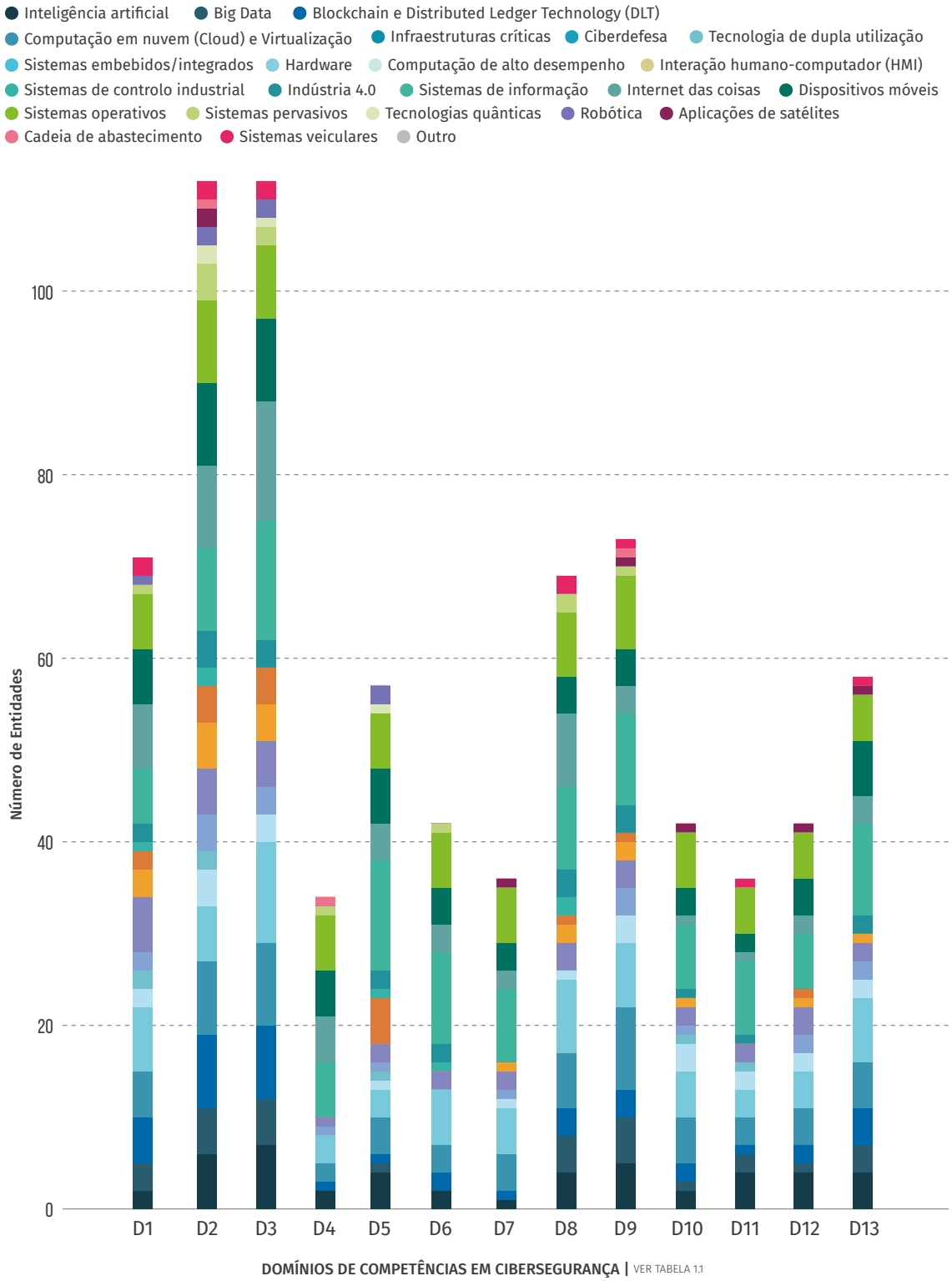
Total das respostas ao questionário on-line relacionando o setor de atividade das entidades participantes com as áreas de aplicações e tecnologias da atividade em cibersegurança.



Ao considerar as áreas de aplicações e tecnologias por domínio de competência em cibersegurança, observa-se uma maior concentração e diversidade no domínio da *Criptologia* e da *segurança e privacidade de dados* (ver Figura 2.11). Outros destaques importantes são as áreas de *redes e sistemas distribuídos* e *engenharia de segurança de software e hardware*. Para o último domínio, o volume de atividade é refletido também na produção científica, tal como é discutido na Secção 2.2.

FIGURA 2.11: APLICAÇÕES E TECNOLOGIAS POR DOMÍNIO DE COMPETÊNCIA - PORTUGAL.

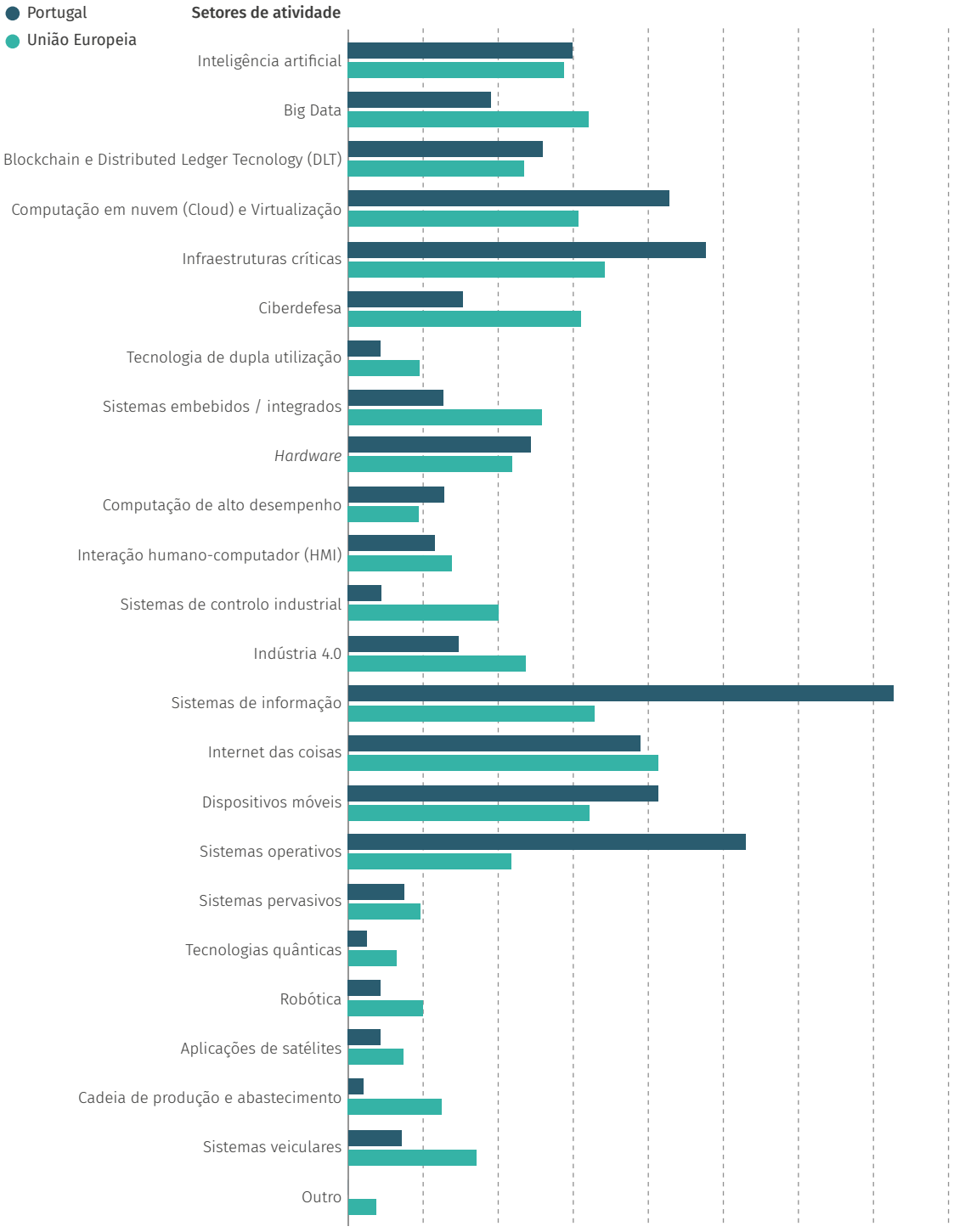
Total das respostas ao questionário on-line relacionando as áreas de aplicações e tecnologias da atividade de entidades nacionais com os domínios de competências em cibersegurança.



Do ponto de vista das áreas de aplicações e tecnologias, a comparação entre a distribuição das respostas dadas ao questionário on-line deste estudo com as respostas ao estudo do ECCC demonstra particularidades interessantes do panorama nacional. Como ilustrado na Figura 2.12, as áreas dos *sistemas de informação* e dos *sistemas operativos* são proporcionalmente bastante mais ativas em Portugal do que na média da União Europeia. Por outro lado, apesar de o volume total não ser significativo, observa-se uma maior concentração de atividade nas áreas ligadas à *Cadeia de produção e abastecimento* e aos *sistemas de controlo industrial* no panorama europeu.

FIGURA 2.12: DISTRIBUIÇÃO COMPARADA DAS ÁREAS DE APLICAÇÕES E TECNOLOGIAS - PORTUGAL E UNIÃO EUROPEIA.

Considera a atividade nacional entre 2017 e 2021 através das respostas ao inquérito on-line e a atividade europeia publicada no estudo do ECCC.



A noção de comunidade de competências passa, também, por identificar a relação entre diferentes entidades com atividade em cibersegurança. Neste sentido, quantificar os memorandos de entendimento assinados pelas entidades que responderam ao questionário on-line com outras organizações, pode dar indicações sobre a dinâmica entre os diferentes setores nacionais com interesse em cibersegurança. Neste sentido, cerca de 34% das entidades afirmam ter assinado, pelo menos, um memorando de entendimento com outras organizações. Destas, 7% afirmam ter assinado entre 4 e 10 memorandos e 1% mais de 10. Ao analisar o número de memorandos pela dimensão da equipa de cibersegurança, observa-se que entidades com equipas relativamente pequenas são responsáveis pela totalidade dos memorandos (ver Figura 2.13). Além disso, continua a observar-se nesta dimensão da análise um maior destaque das instituições de ensino superior e dos centros de investigação (ver Figura 2.14).

FIGURA 2.13: MEMORANDOS POR DIMENSÃO DA EQUIPA DE CIBERSEGURANÇA - PORTUGAL.

Distribuição do número de memorandos pela dimensão das equipas dedicadas às cibersegurança. Por exemplo, cerca de 30% das entidades com equipas compostas por 1 a 3 funcionários dedicados à cibersegurança afirmaram não ter assinado memorandos de cooperação no período entre 2017 e 2021.

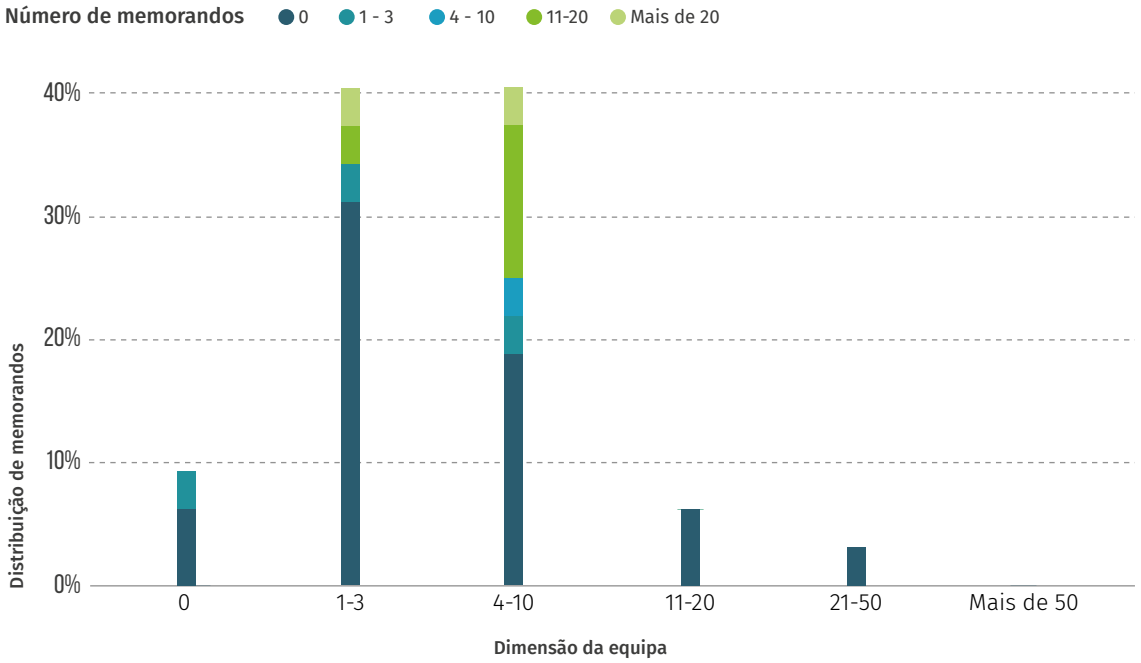
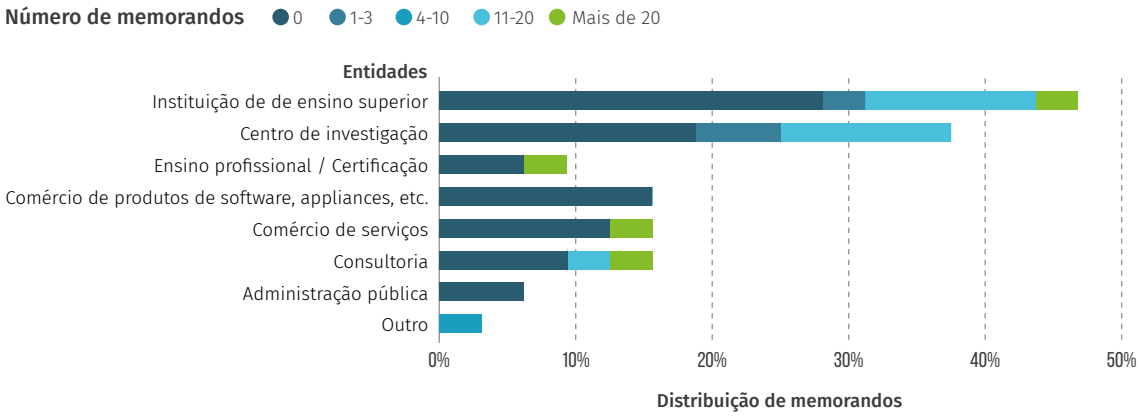


FIGURA 2.14: MEMORANDOS POR TIPO DE ENTIDADE - PORTUGAL

Distribuição do número de memorandos assinados pelo setor de atividade das entidades participantes no período entre 2017 e 2021.

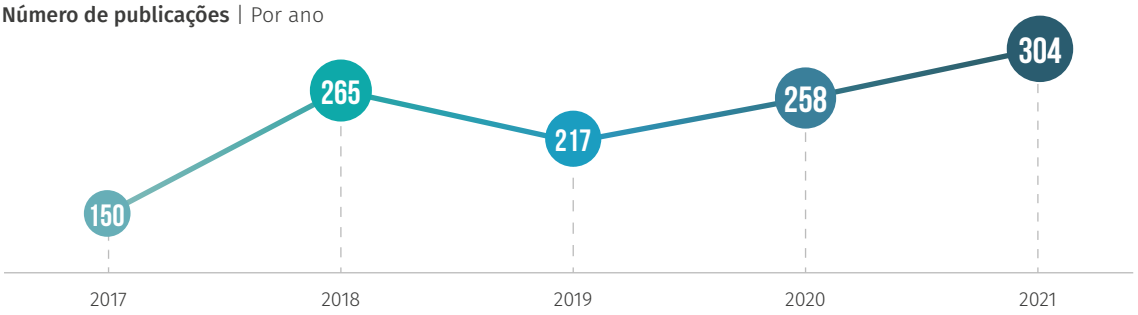


2.2. Panorama Global da Produção Científica em Cibersegurança

Uma das principais dimensões da caracterização das comunidades de competência em cibersegurança em Portugal é sustentada pela identificação e classificação da produção científica nacional. Esta avaliação é justificada pelo número de entidades dedicadas a investigação e inovação, assim como pelos resultados obtidos no período analisado, tanto na forma de captação financeira via programas europeus e nacionais, quanto pelo volume de publicações demonstrado. Neste sentido, o levantamento de dados públicos disponibilizados por repositórios on-line especializados revela que entre janeiro de 2017 e dezembro de 2021, investigadores afiliados a, pelo menos, uma das 37 instituições nacionais publicaram um total de 1139 trabalhos científicos nos diferentes domínios de competências em cibersegurança. Nestes trabalhos, estão incluídos artigos científicos publicados em eventos ou periódicos com revisão por pares, dissertações de mestrado, teses de doutoramento e artigos técnicos. Já em relação aos tipos de entidades responsáveis pela produção científica nacional, há uma concentração quase total nas instituições de ensino superior e nos centros de investigação.

A Figura 2.15 demonstra o volume de publicações anual durante o período considerado neste estudo. Nesta figura, observa-se que apesar de o ano 2017 ter representado um desempenho ligeiramente inferior aos restantes anos, há uma consistência no volume médio da produção científica nacional. Tal como discutido no Capítulo 3, esta regularidade demonstra a capacidade de adaptação das comunidades nacionais à dinâmica dos tópicos de interesse ao longo dos anos.

FIGURA 2.15: PRODUÇÃO CIENTÍFICA EM CIBERSEGURANÇA POR ANO - PORTUGAL.
Considerando a produção agregada de todos os domínios de competências.



Um outro aspeto importante é a distribuição da produção científica total entre as 37 entidades. Tal como demonstrado na Figura 2.16[9], apesar do elevado número de instituições a publicar resultados de trabalhos científicos, cerca de 80% da produção está concentrada em apenas um terço das entidades. Entre elas, destacam-se a Universidade de Coimbra, Universidade do Porto, Universidade de Lisboa, Universidade Nova de Lisboa e Universidade do Minho. Em conjunto, estas cinco instituições são responsáveis por mais de 50% de toda a produção científica nacional no período analisado. Se for considerado o número total de instituições de ensino superior[10] e de centros de investigação[11] nacionais com atividade em áreas relacionadas, observa-se que cerca de 42% das entidades não produziram publicações científicas no período em análise.

9 Um número significativo de publicações, *i.e.*, 269, tem autores com múltiplas afiliações. Nestes casos, para o estudo da concentração da produção científica, a respetiva publicação é contabilizada individualmente para cada entidade.
10 Fonte: https://www.dges.gov.pt/pt/pesquisa_cursos_instituicoes
11 Fonte: https://www.fct.pt/apoios/unidades/unidadesid.phtml.pt

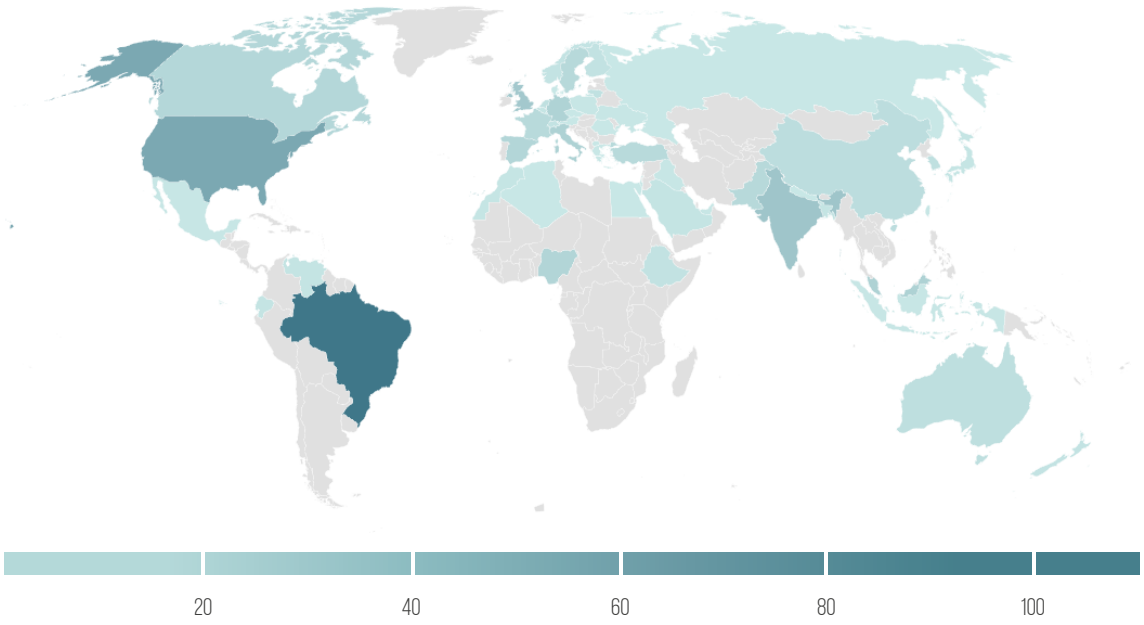
FIGURA 2.16: CONCENTRAÇÃO DE PUBLICAÇÕES POR INSTITUIÇÃO - PORTUGAL.

Representa a concentração total de publicações por instituição no período. Por exemplo, uma instituição nacional publicou 203 documentos entre o período de 2017 e 2021, enquanto 11 instituições publicaram apenas um documento relacionado com cibersegurança no mesmo período (informação omitida no gráfico para melhor representação).

Os dados obtidos permitem também descrever o grau de internacionalização da produção científica nacional. Para isso, considera-se o país de origem das instituições listadas como afiliação de todos os autores das 1139 publicações identificadas. A Figura 2.17 mostra a distribuição comparativa do número de autores por nacionalidade das instituições (sem considerar entidades portuguesas). Nessa distribuição, destacam-se o Brasil (com 111 investigadores), os Estados Unidos da América (com 63 investigadores), a Itália (com 22 investigadores) e a Alemanha (com 21 investigadores). Neste ponto, é interessante observar que os dois principais destaques são países fora da União Europeia, nomeadamente, o Brasil e os Estados Unidos da América. Ainda sobre a Figura 2.17, importa destacar que do total de 3132 autores das 1139 publicações, 898 eram afiliados a, pelo menos, uma instituição portuguesa no momento da respetiva publicação, enquanto 1512 autores eram afiliados a, pelo menos, uma entidade estrangeira [12].

FIGURA 2.17: INTERNACIONALIZAÇÃO.

As zonas mais escuras representam os países-sede de instituições com maior número de autores que colaboraram com investigadores nacionais em publicações científicas no período entre 2017 e 2021.



Ao considerar a distribuição da produção científica entre os domínios de competência em cibersegurança definidos pela ENISA observa-se, em Portugal, uma prevalência da produção na área da *engenharia de segurança de software e hardware* (28% da produção) e na área da *gestão de acesso e identidade* (23% da produção). Como representado na Figura 2.18, há uma diferença significativa entre a concentração da produção científica nacional e a produção agregada dos 37 países participantes do estudo do ECCC. Naquele contexto, a produção científica está mais concentrada no domínio da *Criptologia* e da *engenharia de segu-*

12 Não foi possível identificar a nacionalidade da instituição de afiliação de 722 autores

rança de software e hardware, ambas com aproximadamente 15% das quase 32500 publicações reportadas pelos participantes do estudo. Na distribuição por país, destacam-se a França, a Alemanha e o Reino Unido. Todos com mais de 3 mil publicações nos diferentes domínios de competência. Já Portugal, ocupava a 16ª posição dentre os países analisados.

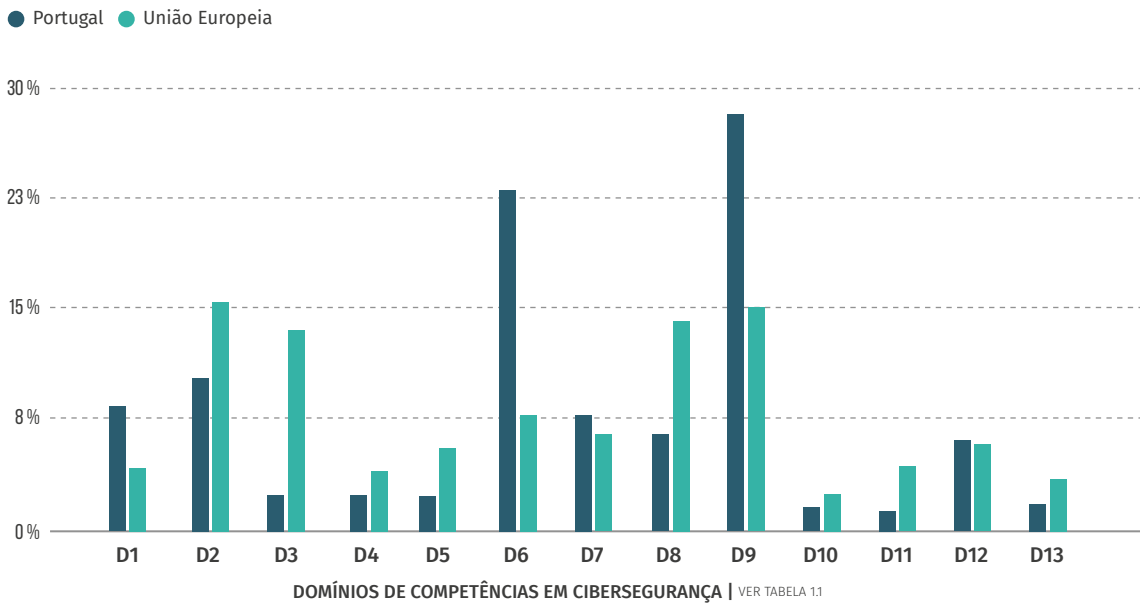
Uma outra análise comparativa entre a produção nacional e o agregado europeu está relacionada com a capacidade de obtenção de patentes a partir da atividade científica. Neste critério, a comunidade de competências nacional atingiu o rácio de uma patente para 94 publicações científicas, enquanto a média europeia equivale a uma patente para 27 publicações. No contexto continental, destacam-se a França e a Finlândia. Contudo, a análise do ECCC já colocava a produção europeia abaixo da expectativa de competitividade internacional, o que faz com que Portugal esteja numa posição ainda mais distante dos objetivos continentais. Neste ponto, é importante ressalvar que o estudo do ECCC não deixa claro qual o período considerado na contabilização de publicações e patentes. Assim, a comparação aqui apresentada dever ser interpretada como um indicador de análises conduzidas em intervalos temporais distintos.

Ainda sobre a distribuição da produção científica por domínio de competência, é possível identificar as áreas relacionadas com Medidas de Segurança, Tecnologia e Aspetos Legais e Gestão de Confiança, Garantia de Segurança e Rastreabilidade como as menos exploradas por investigadores nacionais.

A caracterização detalhada das comunidades de competências nacionais está descrita no Capítulo 3 e segue esta classificação.

FIGURA 2.18: DISTRIBUIÇÃO COMPARADA DA PRODUÇÃO CIENTÍCA POR DOMÍNIO - PORTUGAL E UNIÃO EUROPEIA.

A comparação considera o levantamento da produção nacional entre 2017 e 2021 e a produção europeia reportada no estudo do ECCC.



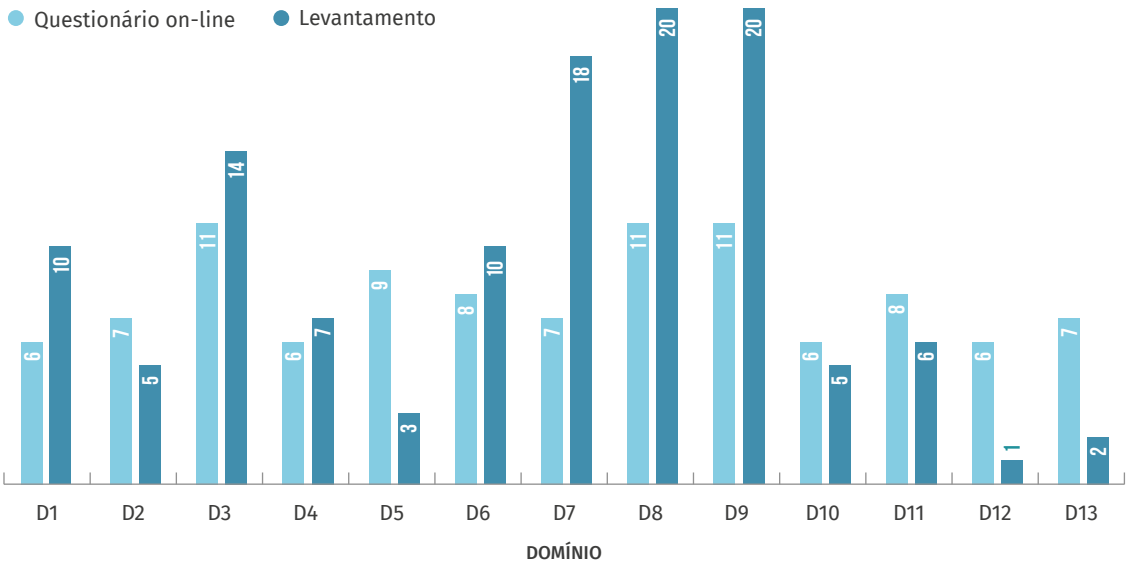
3. CARACTERIZAÇÃO POR DOMÍNIO DE COMPETÊNCIA

3. Caracterização por Domínio de Competência

Esta secção caracteriza detalhadamente a atuação e os resultados obtidos por entidades nacionais em cada um dos domínios de competências em cibersegurança propostos pela ENISA. O resultado desta descrição consiste no retrato de como está organizada a comunidade de competências portuguesa, tendo como referência o contexto europeu de classificação. Para isso, utilizou-se a combinação das respostas ao questionário on-line (ver Anexo A), o registo da produção científica (introduzido na Secção 2.2) e o estudo exploratório de dados de domínio público sobre as entidades empresariais (introduzido na Secção 2.1). Já a Figura 3.1 apresenta o panorama global dos domínios de atuação nacional, tendo por base as respostas ao questionário on-line e o resultado do levantamento exploratório das empresas nacionais. É de notar que apesar do número de entidades que respondeu ao questionário on-line representar cerca de 1/4 do número de empresas objeto do estudo exploratório, a distribuição das atividades segue uma tendência similar nas duas dimensões do estudo. Assim, esta semelhança corrobora a relevância dos resultados obtidos na dimensão do questionário on-line e sustenta a discussão central deste estudo.

FIGURA 3.1: DISTRIBUIÇÃO DAS ATIVIDADES POR DOMÍNIOS.

Considera o total de respostas dadas pelos representantes das entidades participantes no estudo e o levantamento a dados públicos sobre as empresas nacionais com atividade em cibersegurança.



De acordo com as entidades participantes no estudo e os dados obtidos sobre as empresas nacionais, as áreas com maior incidência combinada de atividade global em cibersegurança estão relacionadas com *Segurança e privacidade de dados* (*i.e.*, D03), *Gestão e Governação de Segurança* (*i.e.*, D07), *Redes e sistemas distribuídos* (*i.e.*, D08) e *Engenharia de segurança de software e hardware* (*i.e.*, D09). Apesar de uma parte significativa das entidades participantes no questionário on-line estar dedicada ao ensino superior e à investigação científica, observa-se uma significativa diferença entre a distribuição da Figura 3.1 e da produção científica apresentada na Figura 2.18. Esta diferença é justificada pela alta concentração da produção científica de alguns domínios num conjunto pequeno de instituições. Estas observações são evidenciadas ao longo das próximas secções, onde as particularidades de cada domínio serão apresentadas.

Além disso, é importante observar, neste ponto, um aspeto interessante relacionado com a perceção da taxonomia dos domínios de competências da ENISA pelos intervenientes das empresas que responderam ao questionário on-line. Em entrevistas posteriores à distribuição do questionário, foi possível identificar alguns casos de ambiguidade aquando da indicação dos domínios de atividades aos quais se dedicam. Por exemplo, alguns entrevistados indicaram que classificaram as tarefas e desenvolvimentos ligados à *Gestão de Direitos Digitais* (DRM)[13] nos domínios *Tecnologias e Aspetos Legais* ou *Engenharia de Segurança de*

13 DRM - *Digital Rights Management*

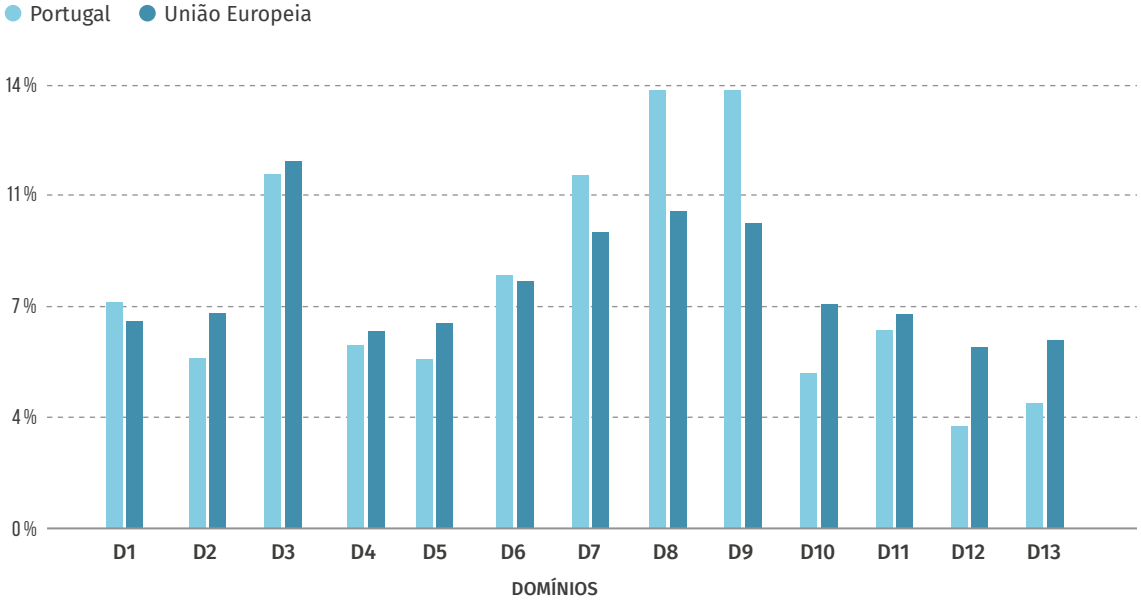
Software e de Hardware, quando a ENISA classifica estas atividades no domínio da *Segurança de Dados e Privacidade*. Outros casos de ambiguidade detetados na fase de entrevista são discutidos nas secções dos respetivos domínios.

Como forma de reduzir o impacto destas ambiguidades no resultado do estudo, o levantamento das publicações científicas em repositórios públicos usa como termos de busca as classes da taxonomia proposta pela ENISA. Abordagem semelhante é adotada no mapeamento das atividades e produtos das entidades empresariais nacionais nos diferentes domínios de competências em cibersegurança. Assim, importa salientar que a discussão apresentada nas próximas secções é resultado de uma análise combinada das diferentes estratégias metodológicas.

No contexto do posicionamento continental da atividade nacional nos diferentes domínios de competência, a Figura 3.2 apresenta a distribuição combinada das respostas ao questionário on-line e o levantamento de dados de domínio público comparada com os resultados obtidos no estudo conduzido pelo ECCC. Nela, é possível observar que apesar de o domínio de maior destaque continental ser a *Segurança de Dados e Privacidade* (i.e., D03), há uma semelhante distribuição global da atividade dos 655 centros de competência analisados com a atuação nacional. A figura mostra também um maior destaque nacional nos domínios da Gestão e Governação de Segurança (i.e., D07), Redes e Sistemas Distribuídos (i.e., D08) e Engenharia de Segurança de Software e Hardware (i.e., D09) quando comparado com a atividade continental.

FIGURA 3.2: DISTRIBUIÇÃO COMPARADA DA ATIVIDADE POR DOMÍNIO - PORTUGAL E UNIÃO EUROPEIA.

A comparação considera a distribuição da atividade nacional entre 2017 e 2021 e a atividade europeia reportada no estudo do ECCC.



3.1. Garantia, Auditoria e Certificação

FIGURA 3.3: D01: DISTRIBUIÇÃO POR SUBDOMÍNIO.

Detalhe da atuação das entidades nacionais no domínio da Garantia, Auditoria e Certificação no período entre 2017 e 2021.

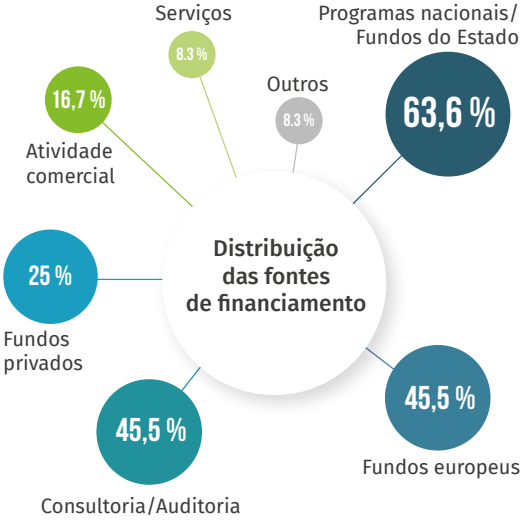
Este domínio de competências em cibersegurança refere-se às metodologias, estruturas e ferramentas que fornecem os mecanismos para obter a confiança de que um sistema, *software*, serviço, processo ou rede que está a funcionar ou foi concebido para funcionar de acordo com os requisitos ou política de segurança definidos.

De acordo com o levantamento efetuado através do questionário on-line, cerca de 6% das entidades possuem algum tipo de atividade no domínio de competências de *Garantia, Auditoria e Certificação* em cibersegurança. Já o levantamento exploratório sobre o tecido empresarial nacional revelou uma proporção de 10% de entidades com algum tipo de atividade neste domínio. Do total de respostas ao questionário, 40% das entidades dedicam-se a atividades de investigação ou inovação tecnológica e 20% ao ensino superior. Importa destacar que neste domínio há uma significativa atividade das entidades nacionais na área de consultoria e auditoria, que corresponde a 28% das respostas obtidas (ver detalhes na Figura 3.4). Todas as atividades são maioritariamente exercidas por instituições de ensino superior e centros de investigação, incluindo consultorias e auditorias. Esta concentração, observada para a maioria dos domínios de competência, demonstra o papel central das instituições de ensino superior e dos centros de investigação no desenvolvimento da cibersegurança em Portugal. Nesta atividade em particular, estão também incluídas entidades dedicadas ao comércio de serviços e à auditoria.

FIGURA 3.4: D01: TIPO DE ATIVIDADE E FONTES DE FINANCIAMENTO.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio da Garantia, Auditoria e Certificação no período entre 2017 e 2021.

0 % Comércio | Serviço | Outro



0% Produtos | Patentes | Outros fundos internacionais

A distribuição dos principais tipos de entidades e atividades neste domínio de competências é refletida na análise das principais fontes de financiamento. Tal como pode ser observado na Figura 3.4, os programas nacionais, os fundos europeus e serviços de consultoria e auditoria suportam a maior parte das atividades. Destacam-se também as entidades que financiam as próprias atividades, em particular, nas entidades de maior dimensão.

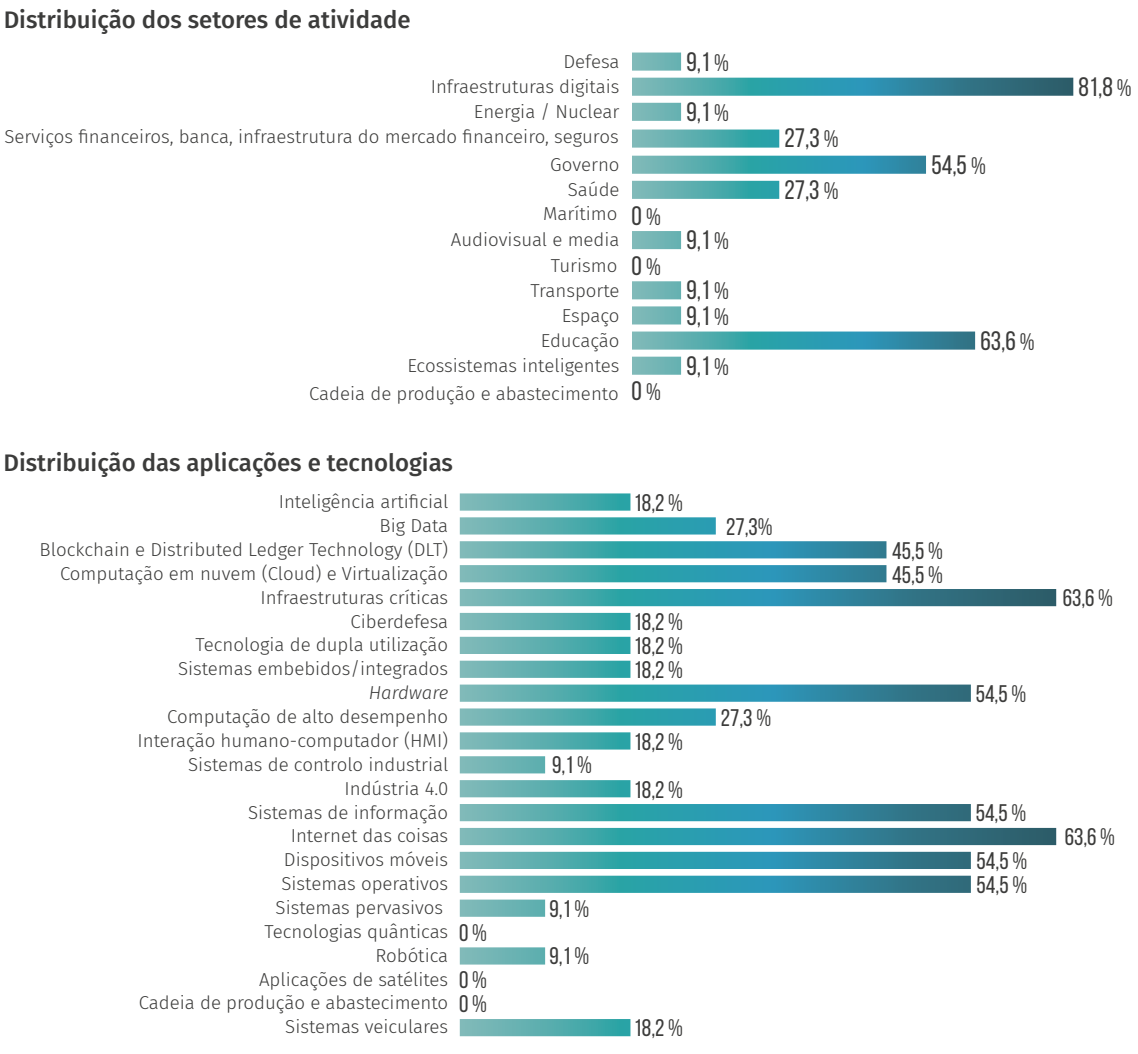
Uma outra dimensão do estudo, que permite a caracterização das comunidades de competências em cibersegurança em Portugal, corresponde ao número de profissionais dedicados a cada domínio da taxonomia europeia. Das entidades que indicaram atividades neste domínio, 55% possuem equipas dedicadas compostas por um a três profissionais, 27% com equipas de quatro a dez profissionais e 18% com equipas de 11 a 20 profissionais.

Ao considerar a distribuição desta atividade pelos subdomínios da taxonomia usada neste estudo (descridos no Anexo B), observa-se uma maior concentração de atuação nas áreas da *avaliação*, *auditoria* e *certificação*[14]. Estes destaques são ratificados pelo resultado do levantamento das atividades do tecido empresarial nacional. Neste caso, porém, o número de entidades com atividade de *auditoria* é ligeiramente maior do que aquelas dedicadas a avaliação de políticas e requisitos de cibersegurança.

As comunidades portuguesas com atuação nas áreas da *Garantia, Auditoria e Certificação* estão divididas, maioritariamente, nos setores de *infraestrutura digital*, *educação* e *governo* (ver Figura 3.5). Ao cruzar esta análise com os tipos de entidade, confirma-se o papel central das instituições de ensino superior na cibersegurança nacional. Tal como descrito no *Estudo sobre o ensino pós-secundário e o ensino superior de cibersegurança em Portugal*, publicado pelo Observatório de Cibersegurança[15], o país testemunha a crescente introdução de conteúdos de cibersegurança em cursos e ciclos de estudo da área das Ciências Informáticas.

FIGURA 3.5: D01: SETORES DA ECONOMIA, APLICAÇÕES E TECNOLOGIAS.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio da Garantia, Auditoria e Certificação no período entre 2017 e 2021. Uma entidade pode atuar em diferentes setores da economia, áreas de aplicações e tecnologias.



14 Do original em inglês *assessment*, *audit* e *certification*.

15 Disponível em https://www.cncs.gov.pt/docs/estudo-ensino-ciberseg-cncs.pdf

Um outro aspeto revelado nesta dimensão do estudo é a importância da administração pública como catalisadora da atividade em cibersegurança, uma vez que cerca de 55% das entidades com atividades neste domínio de competências afirmou ter assinado contratos com o poder público nos últimos cinco anos. Esta relevante colaboração pode estar relacionada com a agenda nacional de modernização da administração pública, que tem sido responsável por investimentos vultuosos em soluções de desmaterialização dos serviços públicos prestados aos cidadãos. Neste sentido, dada a criticidade desses serviços, é natural que as iniciativas de modernização sejam acompanhadas de investimentos em cibersegurança. O tecido industrial tem também um papel relevante, com percentagem idêntica (i.e., 55%) de entidades a afirmar ter assinado contratos com empresas deste setor da economia.

Tanto o papel do poder público, quanto do tecido industrial são ratificados pela análise das aplicações e tecnologias nas quais as atividades deste domínio são empregadas. Como é possível observar na Figura 3.5, o destaque das *infraestruturas críticas*, da I*nternet das coisas* e dos *sistemas de informação* estão alinhados com as atividades e necessidades destes setores.

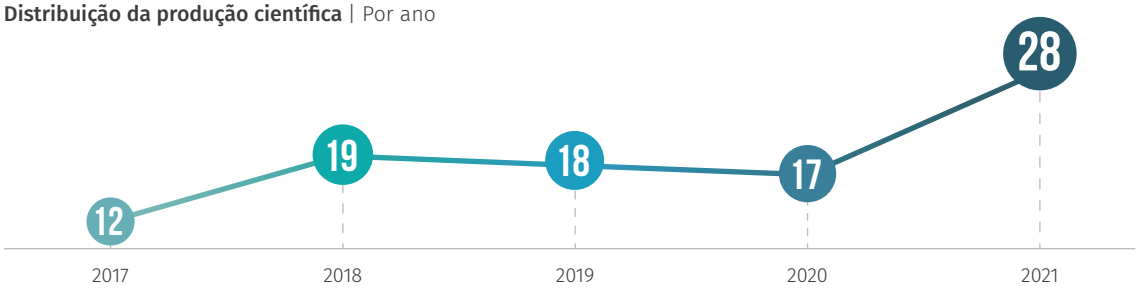
Quando considerada a produção científica nacional no domínio de competências de *Garantia, Auditoria e Certificação*, o estudo identificou um total de 94 publicações da autoria de investigadores ligados a 22 instituições nacionais. A distribuição das publicações entre as diferentes entidades tem como destaques a Universidade de Coimbra, a Universidade do Porto, a Universidade de Aveiro, o Instituto Politécnico de Leiria e a Universidade do Minho. A Figura 3.6 ilustra o grau de concentração da produção científica por instituição. Nesta figura, observa-se que uma instituição (Universidade de Coimbra) publicou 19 artigos neste domínio nos últimos cinco anos, enquanto seis instituições publicaram apenas um cada uma delas.

Por último, a Figura 3.6 descreve a distribuição do total das publicações neste domínio de competências ao longo dos últimos cinco anos. Nesta figura, observa-se um pico de publicações no ano 2021, embora exista regularidade na produção do restante período considerado.

FIGURA 3.6: D01: DISTRIBUIÇÃO DA PRODUÇÃO CIENTÍFICA.

Número de publicações científicas com autores afiliados a instituições nacionais no domínio da Garantia, Auditoria e Certificação.

Distribuição da produção científica | Por ano



Concentração de publicações científicas no domínio da Garantia, Auditoria e Certificação por instituição nacional. Por exemplo, uma instituição nacional foi responsável por 19 publicações no período.

Distribuição da produção científica | Número de publicações por instituição (2017-2021)

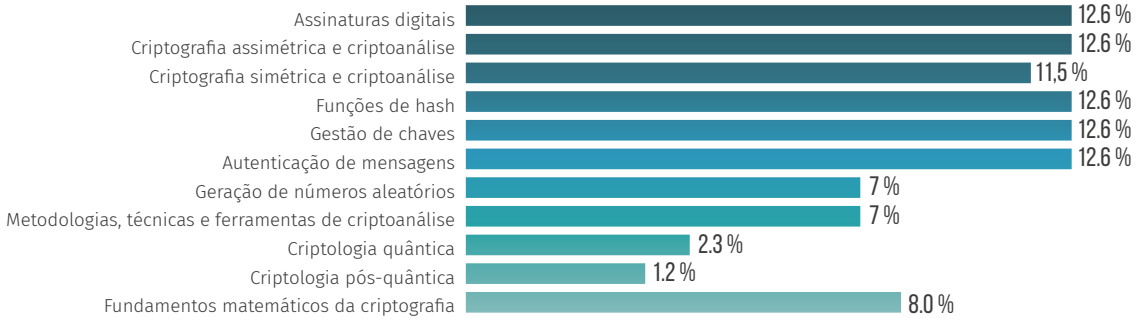
3.2. Criptologia

No contexto da taxonomia europeia para competências em cibersegurança, o domínio da *Criptologia* corresponde à disciplina que estuda a escrita cifrada, o que envolve técnicas de criptografia e de criptoanálise. Neste domínio são incluídos os aspetos matemáticos da Criptologia, os aspetos algorítmicos, a sua implementação técnica e as arquiteturas de infra-estruturas, bem como a implementação de metodologias, técnicas e ferramentas criptanalíticas. Além disso, este domínio também considera a esteganografia digital, que é uma técnica de ocultação de informação num determinado formato digital.

Assim, o domínio é dividido em temas nos quais a comunidade nacional demonstra atividade abrangente. Tal como representado na Figura 3.7, de acordo com as respostas ao questionário on-line, há uma significativa produção em áreas como *assinaturas digitais*, *criptoanálise*, *criptografia simétria e assimétrica*, *gestão de chaves* e *autenticação de mensagens*. Esta concentração é ratificada quando analisados os serviços e produtos comercializados por cerca de 5% das 120 empresas com atividade em cibersegurança analisadas neste estudo. A atuação nacional concentra-se nas atividades de investigação científica e do ensino superior, correspondendo a 68% das entidades que afirmaram possuir competências neste domínio (ver Figura 3.8). Já do ponto de vista da dimensão das equipas dedicadas à Criptologia, 75% das entidades relatam ter entre um e três profissionais, 16% indicam ter entre quatro e dez profissionais e para 9% delas, as equipas contam com 11 a 20 profissionais.

FIGURA 3.7: D02: DISTRIBUIÇÃO POR SUBDOMÍNIO.

Detalhe da atuação das entidades nacionais no domínio da Criptologia no período entre 2017 e 2021.



Alinhado com os tipos de atividades principais, observa-se que as entidades a concentrar uma maior atuação neste domínio de competências são instituições de ensino superior e centros de investigação. Esta caracterização justifica também a predominância de programas nacionais e dos fundos europeus como fontes de financiamento. Como detalhado na Figura 3.7, a distribuição do tipo de financiamento é seguida pelos fundos privados e por serviços de consultoria e auditoria, o que também está alinhado com a proporção de atividades tipicamente relacionadas com estas fontes de financiamento. Importa ressalvar que cerca de 80% das entidades afirmaram ter assinado contratos com a indústria nos últimos cinco anos. Em contrapartida, os contratos com as diferentes instâncias governamentais foram assinados por 50% das entidades com atividade neste domínio. Além disso, 50% das entidades indicou ter firmado memorandos de entendimento com outras organizações no período considerado neste estudo.

Ainda de acordo com as respostas ao questionário on-line, e ilustrado na Figura 3.9, as comunidades nacionais de competências em Criptologia desempenham, maioritariamente, as suas atividades nos setores das *infraestruturas digitais* e da *educação*. Um outro destaque deste domínio são as atividades no setor da *saúde*, que reflete a importância das técnicas criptográficas para o processamento, armazenamento e gestão segura de registos e serviços médicos.

Ao considerar as aplicações e tecnologias que são objetos de desenvolvimento na área, destacam-se os *sistemas de informação*, a *internet das coisas*, os *dispositivos móveis* e os *sistemas operativos*. Impulsionados pela produção científica neste domínio de competências, as *Distributed Ledger Technologies* (DLT), a *computação em nuvem* e os *sistemas de virtualização* também são destaques relevantes a apontar.

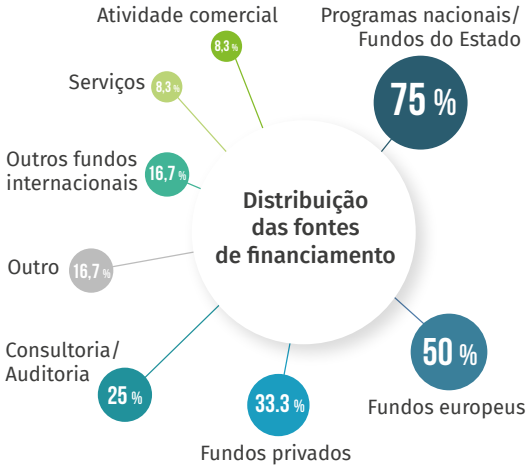
Apesar de o levantamento feito no WIPO não revelar uma ligação direta de nenhuma das 14 patentes identificadas com as áreas deste domínio de competências, uma entidade afirmou ter obtido uma patente relacionada nos últimos cinco anos. Esta discrepância pode estar relacionada com a simplificação das des-

crições públicas para patentes concedidas. Cerca de 17% das entidades também indicou ter obtido registos de *software* no período considerado neste estudo.

FIGURA 3.8: D02: TIPOS DE ATIVIDADE E FONTES DE FINANCIAMENTO.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio de Criptologia no período entre 2017 e 2021.

0 % Comércio | Outro

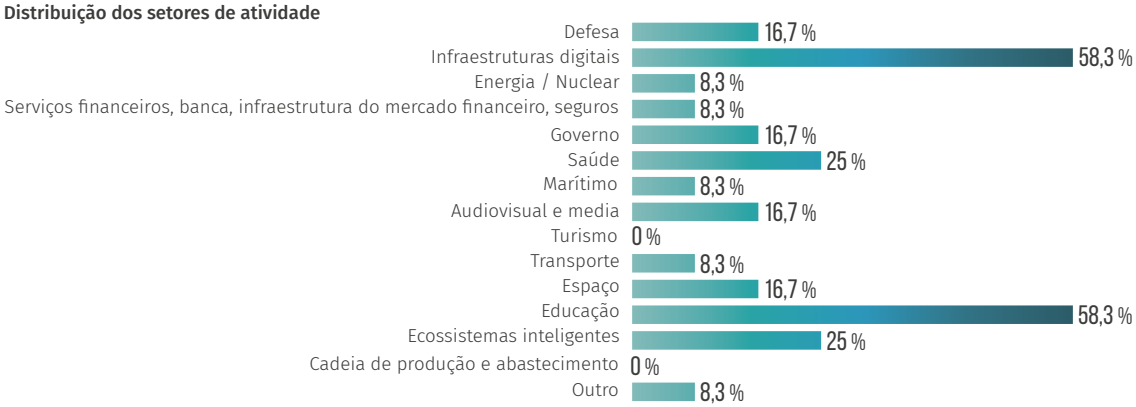


0 % Produtos | Patentes

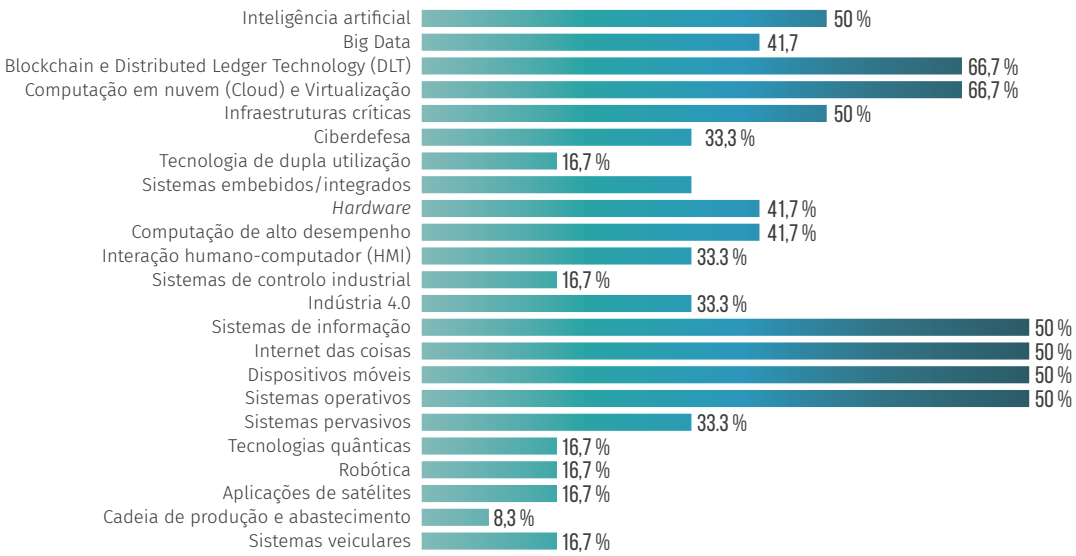
FIGURA 3.9: D02: SETORES DA ECONOMIA, APLICAÇÕES E TECNOLOGIAS.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio de Criptologia no período entre 2017 e 2021. Uma entidade pode atuar em diferentes setores da economia, áreas de aplicações e tecnologias.

Distribuição dos setores de atividade



Distribuição das aplicações e tecnologias



Na vertente das responsabilidades do Estado no domínio da Criptologia, compete especificamente à Agência Nacional de Distribuição (AND) — orgão do Gabinete Nacional de Segurança (GNS) e sob tutela da Autoridade Nacional de Segurança (ANS) — a gestão de material para a proteção criptográfica da Informação Classificada (IC) a nível nacional, seja ele de produção nacional ou confiado à guarda do Estado Português. A AND reune competências na área da Criptologia que lhe permitem garantir a implementação, o controlo de procedimentos adequados e a instalação de canais de comunicação necessários ao cadastro integral, manuseamento, armazenamento e distribuição de material criptográfico em Portugal. São ainda competências da AND, a produção de Normas e Legislação e a monitorização, fiscalização e auditoria de Quebras de Segurança Criptográfica, e de Comprometimentos da Informação Criptográfica.

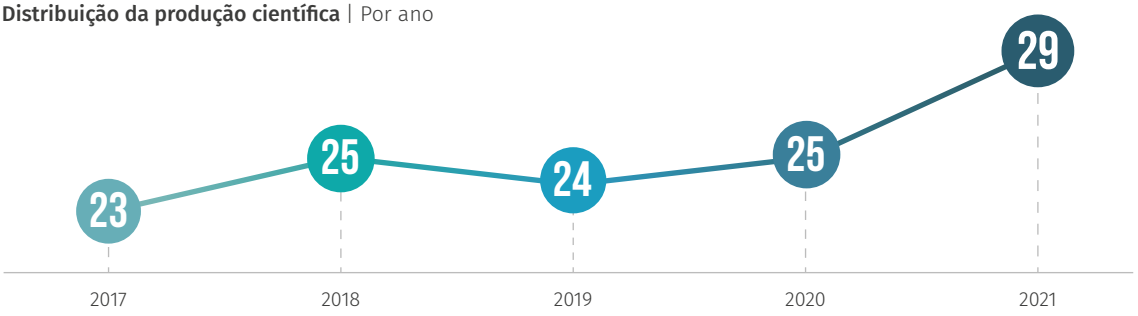
Num importante exemplo de cooperação internacional ligando também indústria e academia, sobressai também a execução do projeto DISCRETION, iniciado em 2020 com financiamento pelo *European Defence Industrial Development Programme* (EDIDP), e que visa a integração de tecnologias de *Software Defined Networks* com a distribuição de chaves quânticas. Um dos resultados esperados deste projeto é o desenvolvimento da primeiro máquina de cifra nacional com capacidade para receber e processar chaves de cifra quânticas.

Na vertente da produção científica, o levantamento de dados em repositórios públicos on-line revela que investigadores de entidades nacionais estiveram envolvidos em 126 publicações de diferentes naturezas nos últimos cinco anos. Este é um dos domínios de competências com maior produção científica nacional. De acordo coma Figura 3.10, existe uma regularidade no volume anual de publicações ao longo do período considerado. A Figura 3.10 demonstra também uma maior distribuição da produção entre instituições com maior volume de publicações, quando comparado com o domínio de competências em *Garantia, Auditoria e Certificação*. Para o domínio de competências em *Criptologia*, seis instituições publicaram, pelo menos, dez artigos no período, destacando-se a Universidade de Lisboa, a Universidade Nova de Lisboa e a Universidade do Porto.

FIGURA 3.10: D02: DISTRIBUIÇÃO DA PRODUÇÃO CIENTÍFICA.

Número de publicações científicas com autores afiliados a instituições nacionais no domínio de Criptologia.

Distribuição da produção científica | Por ano



Concentração de publicações científicas no domínio de Criptologia por instituição nacional. Por exemplo, uma instituição nacional foi responsável por 29 publicações no período.

Distribuição da produção científica | Número de publicações por instituição (2017-2021)

3.3. Segurança de Dados e Privacidade

Este domínio de competências inclui questões de segurança e privacidade relacionadas com dados, a fim de reduzir ou evitar, na fase de conceção de sistemas informáticos, os riscos de violação das propriedades de privacidade, confidencialidade e integridade, sem prejudicar os objetivos funcionais do processamento de dados. É neste domínio onde também se procura impedir a utilização indevida de dados, após o acesso por entidades autorizadas.

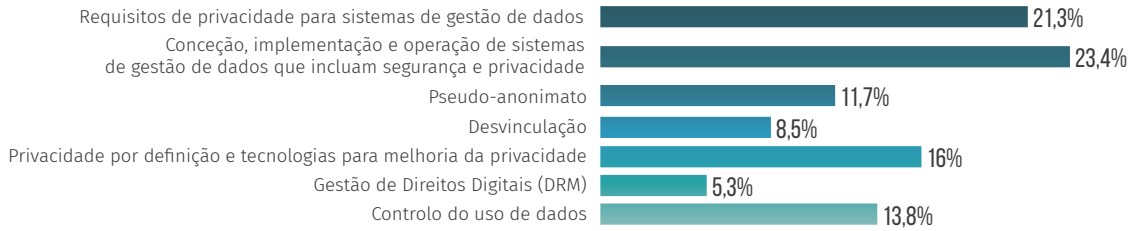
Considerando a vertente do estudo sustentada pelo questionário on-line, o domínio de competências em *Segurança de Dados e Privacidade* corresponde ao grupo com o maior número de entidades atuantes, *i.e.*, mais de 11% das respostas indicam atividade neste domínio. Assim, e tal como nos domínios anteriores, a *investigação científica* e o *ensino superior* representam a maior parte da atividade, cerca de 55%. Entretanto, observa-se aqui uma maior incidência de *prestações de serviços* e *desenvolvimento de soluções* em cibersegurança, responsáveis por mais de 15% e 11% da atividade nacional, respetivamente. Mesmo neste cenário, as instituições de ensino superior e os centros de investigação continuam a concentrar a maior parte da atividade, seguidos pelas consultoras técnicas. Ainda de acordo com os interlocutores dessas entidades, as equipas especializadas em segurança e privacidade de dados são compostas, na sua maioria (68% dos casos) por, no máximo, três profissionais, 27% das entidades possuem equipas de quatro a dez profissionais e 5% empregam entre 21 e 50 especialistas em atividades deste domínio.

Na vertente do estudo sustentada pela análise das áreas de atuação dos associados coletivos das principais associações e polos tecnológicos nacionais, observa-se uma proporção semelhante de empresas com competências neste domínio da cibersegurança. Mais especificamente, cerca de 14% das 120 empresas listam produtos ou serviços ligados, principalmente, à privacidade de dados em diferentes setores e tecnologias. Há uma particular concentração em soluções que garantam o cumprimento do Regulamento Geral sobre a Proteção de Dados (RGPD)[16]. Uma vez que a descrição pública das soluções oferecidas não segue o esquema de classificação europeu, observa-se um natural cruzamento entre diferentes domínios, onde os mais frequentes são a *Gestão de Identidade e Acesso* (*i.e.*, D06), as *Redes e Sistemas distribuídos* (*i.e.*, D07) e a *Engenharia de segurança de software e hardware* (*i.e.*, D09).

Quando avaliada a distribuição das atividades no contexto dos subdomínios da classificação proposta pela ENISA, destacam-se a *conceção, implementação e operação de sistemas de gestão de dados que incluam segurança e privacidade*. Um outro domínio com significativo volume de atuação relaciona-se com os *requisitos de privacidade para sistemas de gestão de dados*. A distribuição entre todos os subdomínios é ilustrada na Figura 3.11.

FIGURA 3.11: D03: DISTRIBUIÇÃO POR SUBDOMÍNIO.

Detalhe da atuação das entidades nacionais no domínio da Segurança de Dados e Privacidade no período entre 2017 e 2021.



Mais uma vez, os programas nacionais e os fundos europeus para o financiamento da investigação científica e a inovação representam as principais fontes de financiamento das entidades nacionais com atuação no domínio da Segurança de Dados e Privacidade. Contudo, um aspeto relevante consiste na ausência de entidades a indicar a *prestação de serviços* e a *comercialização de produtos* em cibersegurança como fonte de financiamento (ver Figura 3.11). Apesar de uma entidade ter indicado a obtenção de patentes no período considerado pelo estudo, nenhuma delas aponta a exploração de patentes como

16 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

fonte de financiamento neste domínio. De acordo com dados do WIPO, uma única entidade privada nacional foi responsável pela obtenção de três registos de patentes ligadas a métodos para a gestão e processamento de dados médicos anonimizados.

Quanto ao panorama dos acordos com organizações externas neste período, o estudo indica que cerca de 33% das entidades participantes assinaram contratos com entidades de natureza pública e 28% com a indústria. Houve também o estabelecimento de memorandos de entendimento entre organizações por 38% dos participantes do estudo.

De forma semelhante ao domínio de competências anterior, os setores de *infraestruturas digitais* e da *educação* concentram o maior número de respostas dadas ao questionário on-line. Observa-se também um volume relativamente alto de atuação nos setores *governamentais* e da *saúde*, o que é corroborado pelo conjunto de patentes previamente descrito. Por outro lado, apesar de o ciclo de investimentos do programa-quadro comunitário para a investigação e inovação que coincidiu com o período considerado neste estudo (*i.e.,* EU H2020) ter a digitalização das infraestruturas de produção e distribuição de energia elétrica como um tema estratégico, nenhuma entidade apontou atividade nesta área. Também a análise dos serviços e produtos oferecidos pelo tecido empresarial nacional não revela atuação significativa neste setor.

FIGURA 3.12: D03: TIPOS DE ATIVIDADE E FONTES DE FINANCIAMENTO.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio da Segurança de Dados e Privacidade no período entre 2017 e 2021.

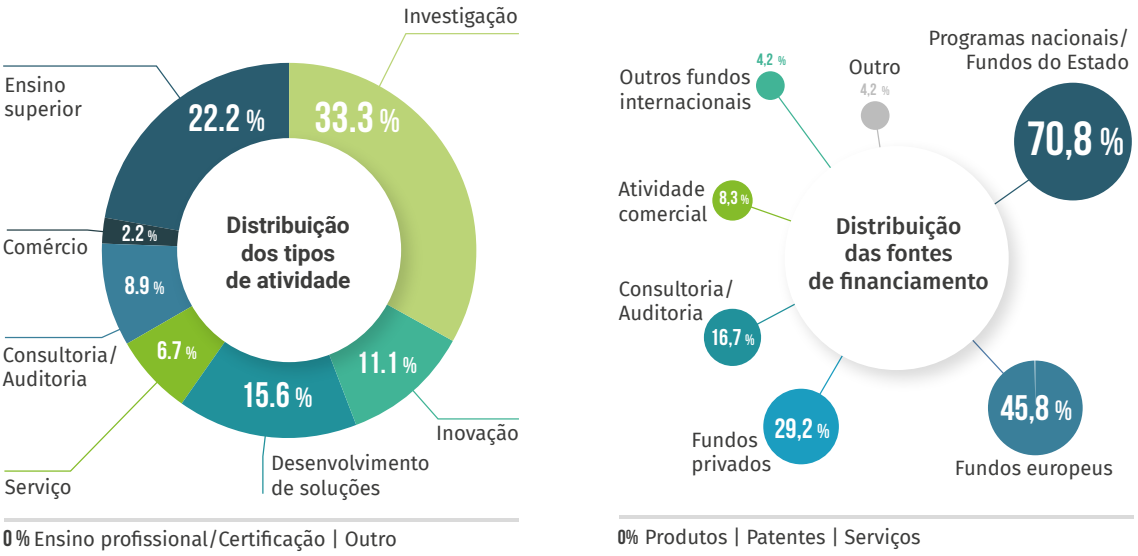
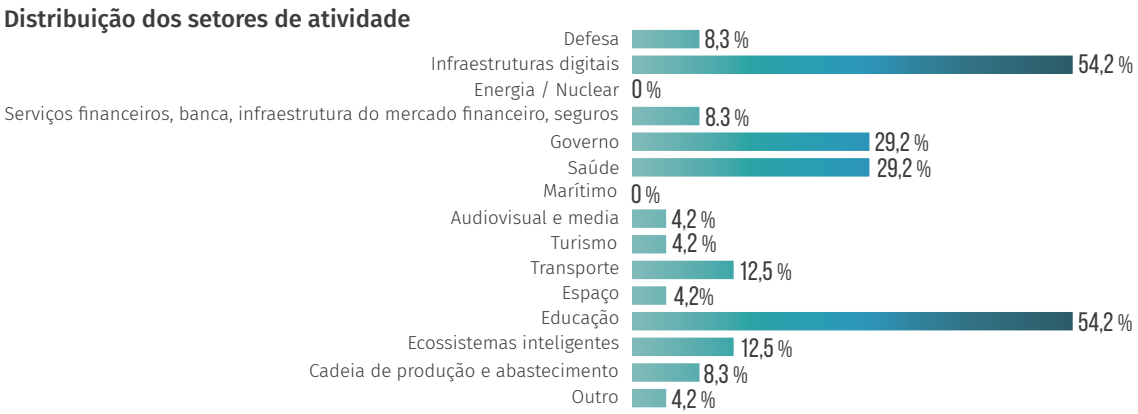
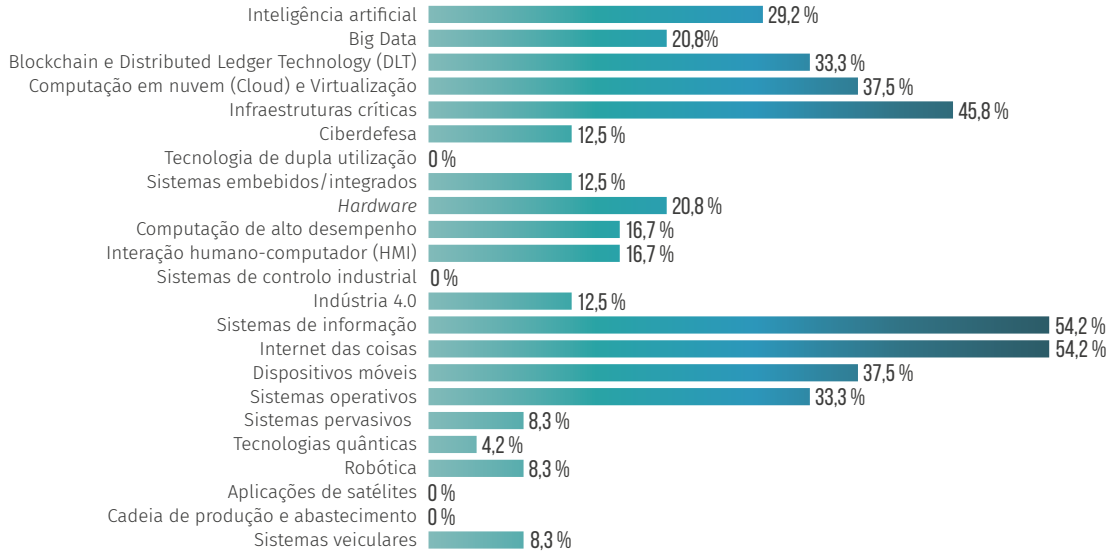


FIGURA 3.13: D03: SETORES DA ECONOMIA, APLICAÇÕES E TECNOLOGIAS.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio da Segurança de Dados e Privacidade no período entre 2017 e 2021. Uma entidade pode atuar em diferentes setores da economia, áreas de aplicações e tecnologias.



Distribuição das aplicações e tecnologias



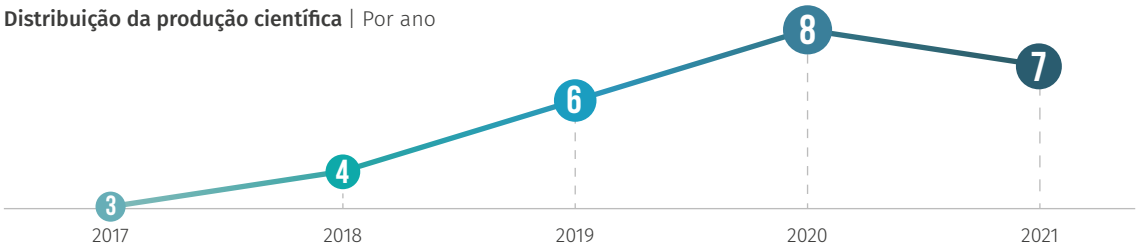
Já nas tecnologias e áreas de aplicações onde há uma maior produção nacional destacam-se os *sistemas de informação* e a *internet das coisas*. Apesar de ser uma área com reconhecido desenvolvimento em Portugal, as atividades de cibersegurança em *sistemas de controlo industrial* representam uma ausência notável na vertente de questionário on-line do estudo. A análise das ofertas de serviços e produtos pelo tecido empresarial não altera esta observação, já que apenas duas empresas descrevem algum tipo de competência nesta área.

Apesar de um volume total (*i.e.*, 27) relativamente baixo quando comparado com outros domínios de competências, observa-se uma evolução constante no número de publicações de caráter científico (ver Figura 3.14). Consequentemente, nenhuma instituição apresenta um volume significativo de publicações neste domínio, cabendo à Universidade de Lisboa e à Universidade do Porto a maior concentração de publicações no período, com cinco e quatro publicações, respetivamente.

FIGURA 3.14: D03: DISTRIBUIÇÃO DA PRODUÇÃO CIENTÍFICA.

Número de publicações científicas com autores afiliados a instituições nacionais no domínio da Segurança de Dados e Privacidade.

Distribuição da produção científica | Por ano



Concentração de publicações científicas no domínio da Segurança de Dados e Privacidade por instituição nacional. Por exemplo, uma instituição nacional foi responsável por seis publicações no período.

Distribuição da produção científica | Número de publicações por instituição (2017-2021)

3.4. Tratamento/Resposta a Incidentes Operacionais e Ciência Forense Digital

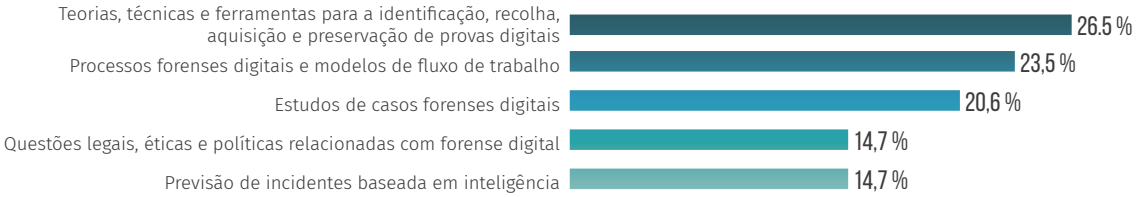
Este domínio de competências em cibersegurança refere-se às teorias, técnicas, ferramentas e processos para a identificação, recolha, aquisição e preservação de provas digitais. Tendo em conta as respostas obtidas via questionário on-line, o domínio que engloba as tarefas de *tratamento e resposta de incidentes operacionais* e *forense digital* corresponde a um dos grupos com menor atuação das entidades portuguesas. Pouco mais de 6% das entidades participantes do estudo indicou algum tipo de atividade nestas áreas. Este é um indicador preocupante quando posto em perspetiva, uma vez que tem havido um aumento significativo no volume de incidentes de cibersegurança e nos números dos indicadores de cibercrime em Portugal[17].

Mesmo quando consideradas as atividades em cibersegurança listadas pelo tecido empresarial e caracterizadas via levantamento on-line, a proporção não é diferente. Cerca de 7% das 120 empresas com atividade em cibersegurança anunciam algum tipo de produto ou serviço neste domínio de competências. Na sua maior parte, estas empresas dedicam a sua atividade à deteção e resposta a incidentes de segurança em sistemas de informação de grande escala. Aqui, observa-se também a interseção com outros domínios de competências, nomeadamente, *Gestão e Governação de Segurança* (*i.e.*, D07), *redes e sistemas distribuídos* (*i.e.*, D08) e *engenharia de segurança de software e hardware* (*i.e.*, D09).

Entre as entidades com atuação neste domínio, destacam-se, com igual volume, aquelas dedicadas à *investigação científica* e à *prestação de serviços*. É de notar que este é um dos poucos domínios onde o ensino superior não aparece entre os dois principais tipos de atividade (ver distribuição na Figura 3.15). Ainda assim, as instituições de ensino superior e os centros de investigação concentram a maior parte das respostas para este domínio de competências. Globalmente, as equipas de especialistas nas atividades deste domínio são compostas, no máximo, por três profissionais (*i.e.*, em 75% das entidades). As restantes entidades reportaram equipas entre quatro e dez profissionais.

FIGURA 3.15: D04: DISTRIBUIÇÃO POR SUBDOMÍNIO.

Detalhe da atuação das entidades nacionais no domínio do Tratamento/Resposta de Incidentes Operacionais e Forense Digital no período entre 2017 e 2021.



Ao analisar como a atuação destas entidades está distribuída entre os diferentes subdomínios, três áreas merecem destaque, nomeadamente:

- Teorias, técnicas e ferramentas para a identificação, recolha, aquisição e preservação de provas digitais;
- Processos forenses digitais e modelos de fluxo de trabalho;
- Estudos de casos forenses digitais.

Como destacado na Figura 3.16, os *programas nacionais* para a investigação e inovação são as principais fontes de financiamento deste domínio de atividades. Do ponto de vista do número de entidades financiadas, a lista com as fontes de recursos mais relevantes é seguida pelos *fundos europeus*, por *fundos privados* e por serviços de *consultoria e auditoria*. Ainda sobre a forma como as entidades financiam desenvolvimentos nesta área, 25% das respostas indicam a assinatura de contratos com a indústria nos últimos cinco anos e cerca de 30% indicou contratos firmados com o poder público no mesmo período. Mais uma vez, apesar de uma entidade afirmar ter obtido uma patente relacionada com o domínio, não há indicação de financiamento por exploração de propriedade intelectual. Além disso, apenas duas entidades relataram ter firmado memorandos de entendimento com outras organizações.

17 Fonte: Relatório Riscos & Conflitos 2021 - Cibersegurança em Portugal (CNCS) - https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurança-cncs.pdf

Apesar de não representar a atividade principal, o setor da educação é apontado como o maior destino dos esforços nesta área, onde é maioritariamente aplicado aos sistemas *de informação*, *internet das coisas*, *sistemas operativos* e *sistemas pervasivos*. O setor da administração pública também se destaca como o segundo para o qual as atividades neste domínio de competência se concentram.

FIGURA 3.16: D04: TIPOS DE ATIVIDADE E FONTES DE FINANCIAMENTO.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio do Tratamento/Resposta de Incidentes Operacionais e Forense Digital no período entre 2017 e 2021.

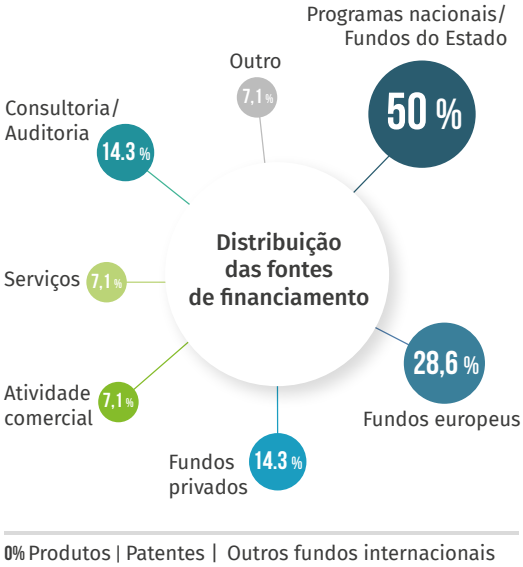
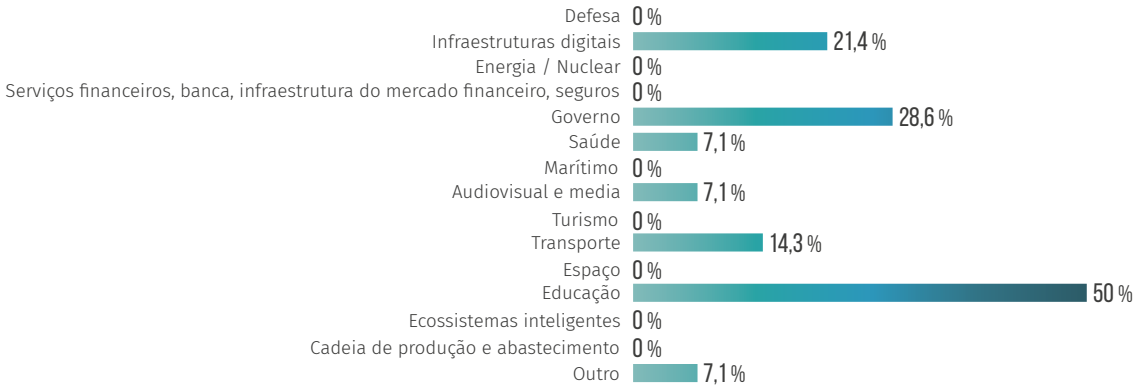


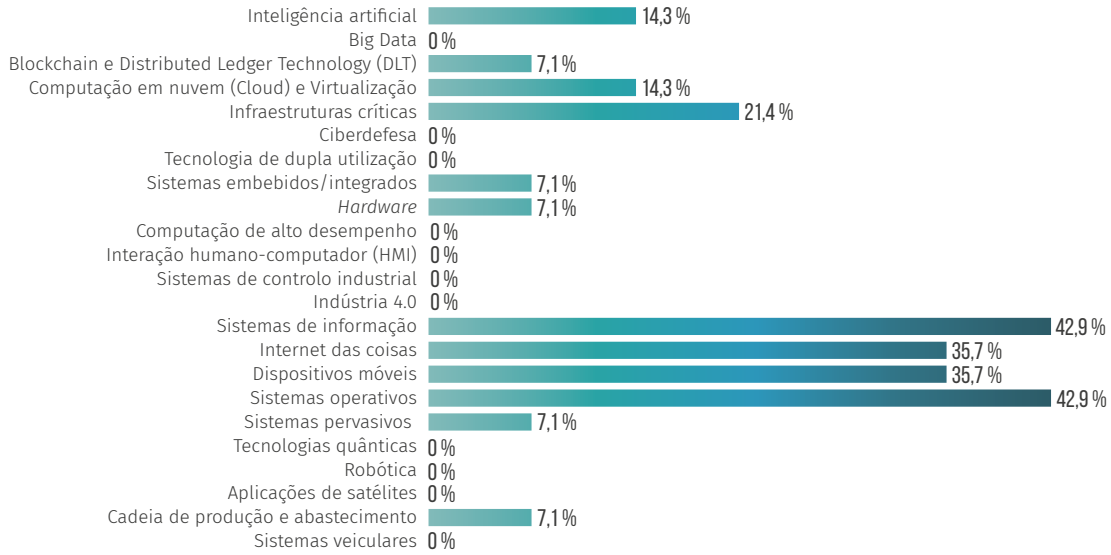
FIGURA 3.17: D04: SETORES DA ECONOMIA, APLICAÇÕES E TECNOLOGIAS.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio do Tratamento/Resposta de Incidentes Operacionais e Forense Digital no período entre 2017 e 2021. Uma entidade pode atuar em diferentes setores da economia, áreas de aplicações e tecnologias.

Distribuição dos setores de atividade



Distribuição das aplicações e tecnologias

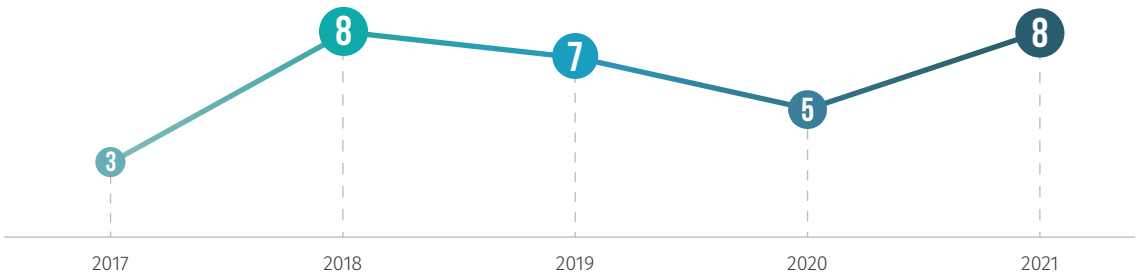


Na vertente da produção científica nacional, o domínio de competências do *tratamento e resposta de incidentes operacionais* e da *forense digital* totalizou 31 publicações ao longo dos últimos cinco anos. Apesar de não haver uma diferença significativa, com exceção de 2017, a produção nacional é praticamente idêntica (ver Figura 3.18). Também não se observa uma concentração significativa da produção por entidades. Mesmo assim, é importante destacar o Instituto Politécnico de Leiria e a Universidade do Porto como as principais fontes de produção científica neste domínio.

FIGURA 3.18: D04: DISTRIBUIÇÃO DA PRODUÇÃO CIENTÍFICA.

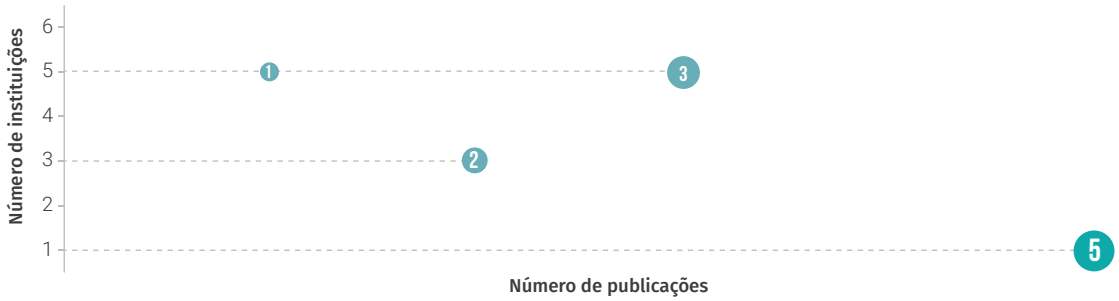
Número de publicações científicas com autores afiliados a instituições nacionais no domínio do Tratamento/Resposta de Incidentes Operacionais e Forense Digital.

Distribuição da produção científica | Por ano



Concentração de publicações científicas no domínio do Tratamento/Resposta de Incidentes Operacionais e Forense Digital por instituição nacional. Por exemplo, uma instituição nacional foi responsável por cinco publicações no período.

Distribuição da produção científica | Número de publicações por instituição (2017-2021)

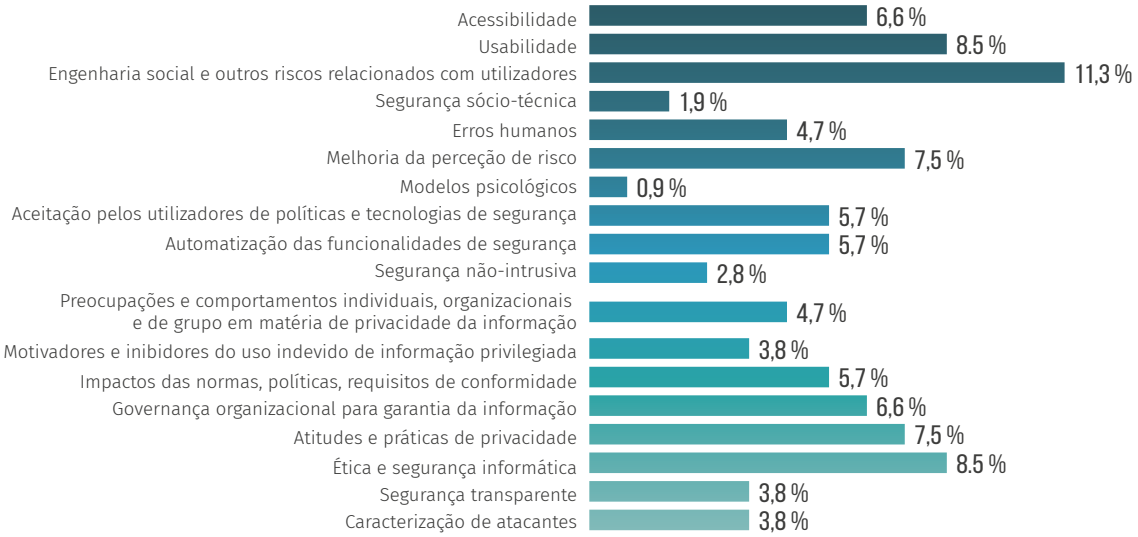


3.5. Fatores Humanos

No contexto da classificação europeia para os domínios de competência, os *Fatores Humanos* lidam com a interação entre ética, leis relevantes, regulamentos, políticas, normas, psicologia e o ser humano, dentro do domínio da cibersegurança. De acordo com os dados obtidos via questionário on-line, cerca de 9% das entidades afirmam possuir competências e desenvolver atividades neste domínio. Dada a natureza das atividades enquadradas neste domínio, há um número proporcionalmente reduzido de empresas a listar serviços ou produtos relacionados. De acordo com o levantamento feito no tecido empresarial nacional, menos de 3% das entidades consultadas listam atividades no domínio.

FIGURA 3.19: D05: DISTRIBUIÇÃO POR SUBDOMÍNIO.

Detalhe da atuação das entidades nacionais no domínio dos Fatores Humanos no período entre 2017 e 2021.



Considerando as respostas ao questionário on-line, estas entidades dedicam atividades relacionadas maioritariamente (*i.e.*, 50%) com a investigação científica e com o ensino superior (ver Figura 3.20). Destaques interessantes neste domínio são as atividades de *inovação* e de *desenvolvimento de soluções*, onde mais de 11% das entidades indicam atividades em cada área. Na sua maioria (*i.e.*, 75%), as entidades possuem equipas de especialistas neste domínio compostas por até três profissionais. Nas restantes, as equipas são de quatro a dez especialistas dedicados aos Fatores Humanos da Cibersegurança.

A classificação deste domínio de competências, segundo a ENISA, concentra um grande número de subdomínios, tal como é ilustrado na Figura 3.19. Nesta figura, destacam-se desenvolvimentos nas áreas de:

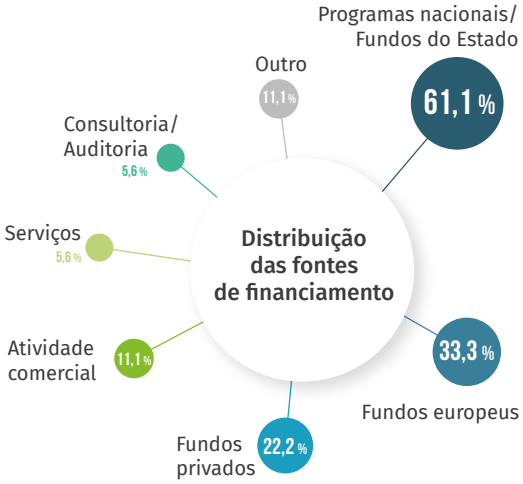
- Engenharia social e outros riscos relacionados com utilizadores;
- Usabilidade;
- Ética e segurança informática;
- Melhoria da perceção de risco.

Quando consideradas as fontes de financiamento para as atividades neste domínio de competências, destacam-se, principalmente, os programas nacionais de investigação e inovação. Em número de respostas, esta fonte de financiamento é seguida pelos fundos europeus e pelos fundos privados. Alinhado com os tipos de atividades ilustrados na Figura 3.20, mais de 30% das entidades participantes indicou envolvimento em projetos de inovação nos últimos cinco anos. A percentagem de entidades com participação em projetos europeus e nacionais é de 25% e 31%, respetivamente. Ainda sobre as fontes de financiamento no período considerado neste estudo, 25% dos participantes indicou ter firmado contratos com entidades da indústria, enquanto cerca de 20% indicou parcerias formais com órgãos do poder público.

FIGURA 3.20: D05: TIPOS DE ATIVIDADE E FONTES DE FINANCIAMENTO.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio dos Fatores Humanos no período entre 2017 e 2021.

0 % Comércio | Outro

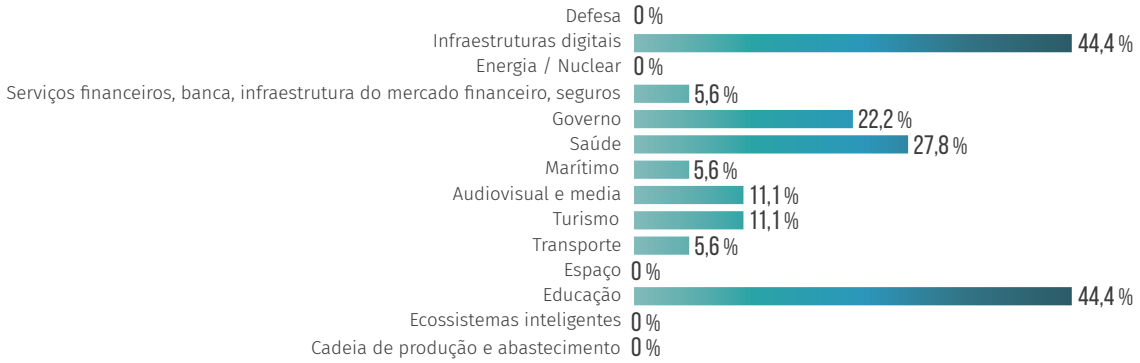


0% Produtos | Patentes | Outros fundos internacionais

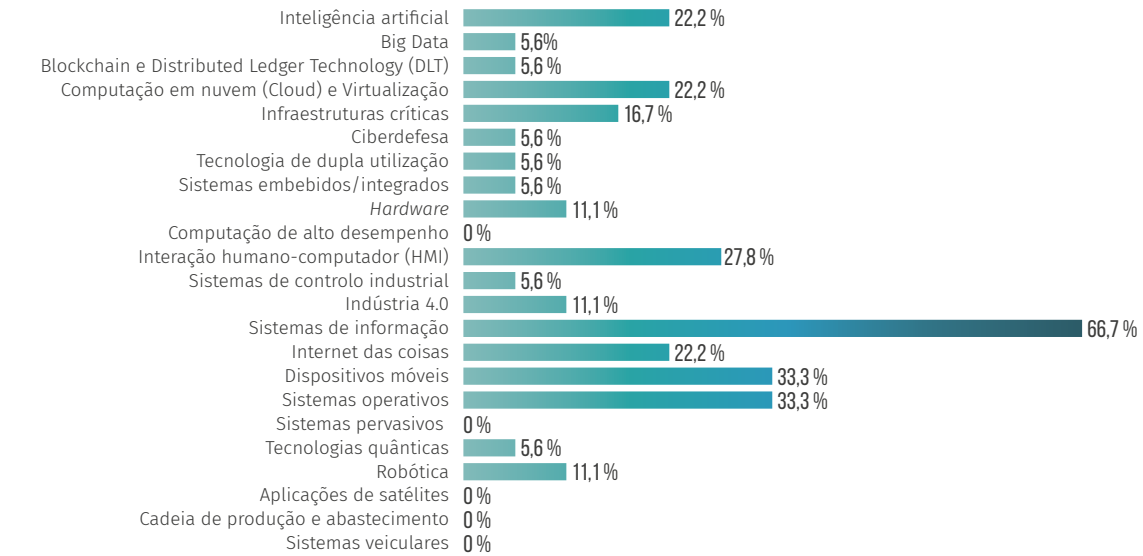
FIGURA 3.21: D05: SETORES DA ECONOMIA, APLICAÇÕES E TECNOLOGIAS.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio dos Fatores Humanos no período entre 2017 e 2021. Uma entidade pode atuar em diferentes setores da economia, áreas de aplicações e tecnologias.

Distribuição dos setores de atividade



Distribuição das aplicações e tecnologias

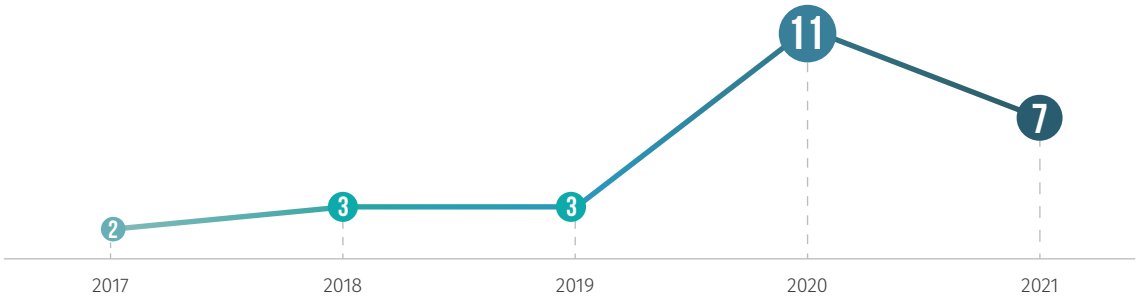


Do ponto de vista da divulgação de resultados na forma de publicações científicas, as comunidades nacionais de competências em *Fatores Humanos* da Cibersegurança produziram 26 trabalhos nos últimos cinco anos. Entre elas, destacam-se a Universidade de Évora, o Instituto Universitário de Lisboa, o Instituto Superior de Tecnologias Avançadas do Porto e o Instituto Superior de Tecnologias Avançadas de Lisboa. Estas instituições foram responsáveis por cerca de 45% da produção científica nacional. Além disso, como ilustrado na Figura 3.22, houve um aumento no volume de publicações nos últimos dois anos do período considerado neste estudo.

FIGURA 3.22: D05: DISTRIBUIÇÃO DA PRODUÇÃO CIENTÍFICA.

Número de publicações científicas com autores afiliados a instituições nacionais no domínio dos Fatores Humanos.

Distribuição da produção científica | Por ano



Concentração de publicações científicas no domínio dos Fatores Humanos por instituição nacional. Por exemplo, uma instituição nacional foi responsável por quatro publicações no período.

Distribuição da produção científica | Número de publicações por instituição (2017-2021)

3.6. Gestão de Identidade e Acesso

Este domínio de competências em cibersegurança abrange processos e políticas envolvidos na gestão do ciclo de vida dos atributos e dos metadados opcionais em identidades conhecidas num determinado cenário. Além disso, também considera aspetos de gestão de acesso, incluindo autenticação, autorização e controlo de acesso de indivíduos e objetos inteligentes a recursos. Estas preocupações podem incluir elementos físicos e digitais dos sistemas de autenticação e aspetos legais relacionados com a conformidade e a aplicação da lei.

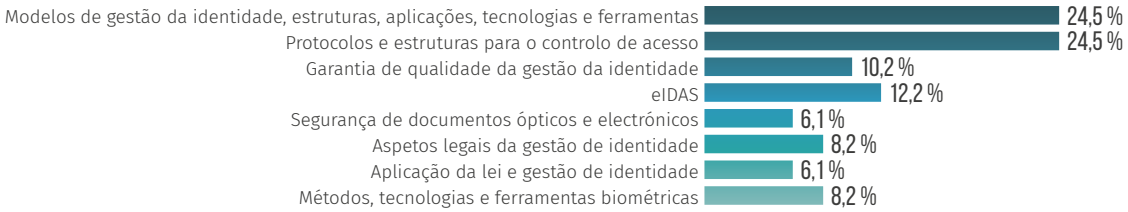
De acordo com o levantamento sobre as competências em cibersegurança do tecido empresarial nacional, aproximadamente, 10% dos associados coletivos de, pelo menos, uma das entidades listadas na Tabela 2.1, indicam, nas suas respetivas páginas da Internet, alguma atividade no domínio da *Gestão de Identidade e acesso*. Por ser, do ponto de vista comercial, um domínio responsável por tecnologias que suportam diferentes produtos e serviços, observa-se clara intersecção com outros domínios da taxonomia adotada neste estudo. Dentre eles, destacam-se a *Segurança de Dados e Privacidade* (*i.e.*, D03) e a *Gestão e Governação de Segurança* (*i.e.*, D07).

Já os dados obtidos via questionário on-line, revelam que cerca de 8% das entidades participantes do estudo desenvolvem algum tipo de atividade no domínio de competências relacionado com a *Gestão de Identidade e Acesso*. Deste total, mais de 38% dedicam-se a atividades ligadas ao ensino superior, 33% a investigação científica e cerca de 14% a atividades de serviços. No que respeita as subáreas deste domínio, destacam-se as seguintes:

- Modelos de gestão da identidade, estruturas, aplicações, tecnologias e ferramentas;
- Protocolos e estruturas para o controlo de acesso;
- eIDAS - electronic IDentification, Authentication and trust Services;
- Garantia de qualidade da gestão da identidade.

FIGURA 3.23: D06: DISTRIBUIÇÃO POR SUBDOMÍNIO.

Detalhe da atuação das entidades nacionais no domínio da Gestão de Identidade e Acesso no período entre 2017 e 2021.



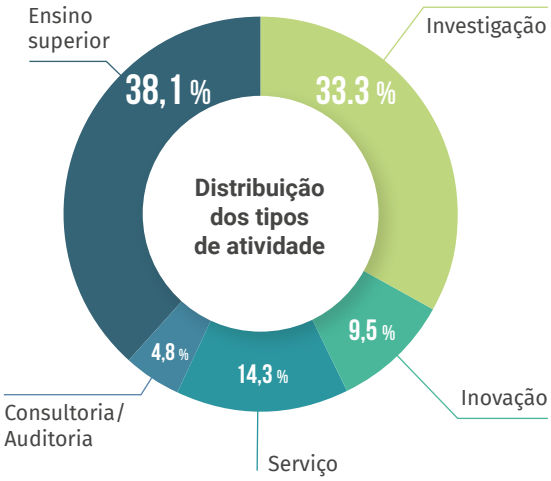
Ainda de acordo com as respostas ao questionário on-line, há uma quase total concentração do financiamento por via de programas nacionais ou fundos europeus para a investigação e inovação. Este perfil é constatado pela inexistência de contratos com entidades públicas, assim como de registos de *software* ou de patentes relacionados. Relativamente a contratos com a indústria, este ponto foi apontado por apenas uma entidade como fonte de financiamento. Ao comparar esta informação com a distribuição das atividades por setores (ver Figura 3.25), é evidente o caráter académico dos desenvolvimentos nacionais nesta área de competências da cibersegurança.

Entretanto, apesar de nenhuma entidade ter apontado a obtenção de registos de patente, o levantamento na base de dados do WIPO revelou que duas instituições do setor privado nacional obtiveram três patentes no âmbito deste domínio nos últimos cinco anos. Mais especificamente, uma das patentes introduz inovação em documentos de identificação virtuais e as restantes implementam procedimentos de *login* com um clique.

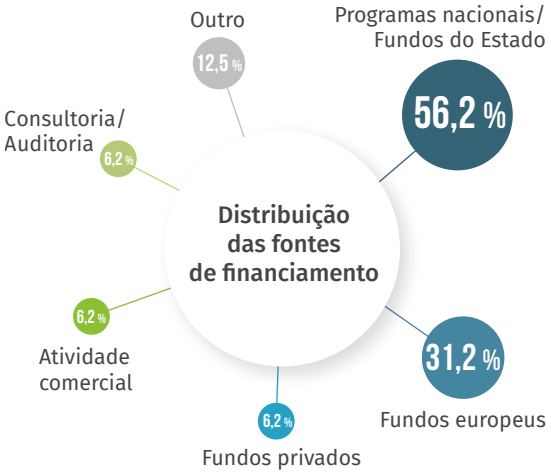
Já do ponto de vista da força de trabalho envolvida nos desenvolvimentos ligados a este domínio, as entidades participantes do estudo indicaram que, na sua maior parte (*i.e.*, 76%) empregam equipas especializadas de até três profissionais. Em 16% dos casos, as equipas possuem entre quatro e dez profissionais e, para 8% das entidades, as equipas são formadas por 11 a 20 pessoas.

FIGURA 3.24: D06: TIPOS DE ATIVIDADE E FONTES DE FINANCIAMENTO.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio da Gestão de Identidade e Acesso no período entre 2017 e 2021.



0 % Ensino profissional/Certificação | Serviço | Outro

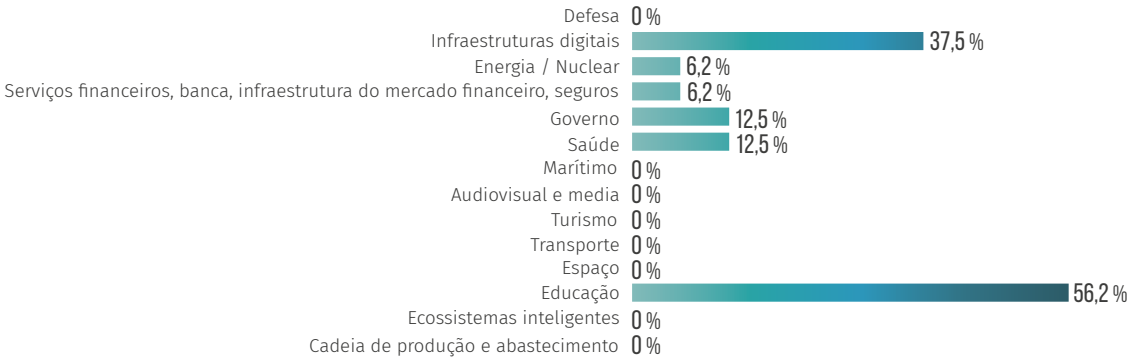


0% Produtos | Patentes | Serviços | Outros fundos internacionais

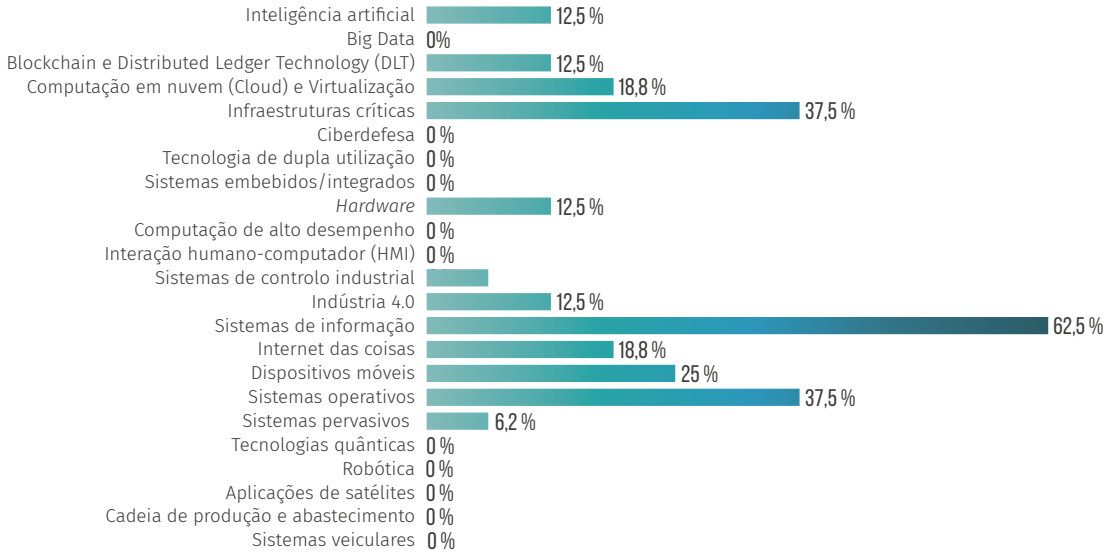
FIGURA 3.25: D06: SETORES DA ECONOMIA, APLICAÇÕES E TECNOLOGIAS.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio da Gestão de Identidade e Acesso no período entre 2017 e 2021. Uma entidade pode atuar em diferentes setores da economia, áreas de aplicações e tecnologias.

Distribuição dos setores de atividade



Distribuição das aplicações e tecnologias



Um aspeto interessante do levantamento feito em repositórios on-line de publicações científicas é que o resultado confirma, estatisticamente, a distribuição indicada pelas entidades participantes no estudo quanto às aplicações e tecnologias objetos dos seus desenvolvimentos. Tal como ilustrado na Figura 3.25, há uma maior concentração nos desenvolvimentos relacionados com os *sistemas de informação*, as *infraestruturas críticas* e os *sistemas operativos*.

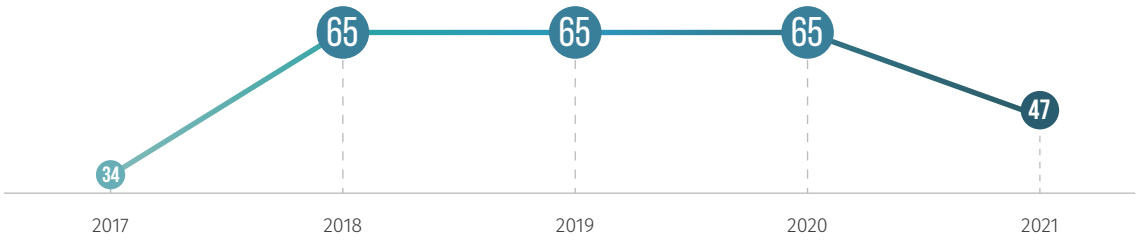
A dimensão do estudo sobre a produção científica revelou que este domínio concentra um dos maiores números de trabalhos publicados nos últimos cinco anos, totalizando 276 publicações. Neste ponto, é importante salientar que uma das principais razões para este maior volume relativo de produção é a natureza dos trabalhos neste domínio, tipicamente orientados à investigação aplicada em detrimento da investigação fundamental, como observado noutros domínios de competências (*e.g.*, criptologia). Um outro fator determinante para o destaque das comunidades nacionais neste domínio, está relacionado com a abrangência de alguns termos de busca usados para identificar a produção científica. Por exemplo, o termo *controlo de acesso* aparece relacionado com um grande e variado conjunto de aplicações e tecnologias de interesse significativo para as comunidades académicas nacionais, o que faz com que seja responsável por mais de 30% das publicações identificadas neste domínio. Além disso, uma publicação que tenha como temas o controlo de acesso em redes de computadores aparecerá em ambos os domínios de competências (*i.e.*, D06 e D08), embora o volume global discutido na Secção 2.2 contabilize apenas uma única entrada. É importante também destacar que os termos de pesquisa foram definidos a partir da taxonomia da ENISA.

Quando considerada a distribuição destas publicações ao longo dos cinco anos considerados neste estudo, observa-se uma regularidade na produção nacional, particularmente, entre os anos 2018 e 2021 (ver Figura 3.26). Já a distribuição entre instituições demonstra um grande volume de publicações, em especial, de investigadores ligados à Universidade do Porto, à Universidade de Coimbra, à Universidade de Lisboa, à Universidade Nova de Lisboa e ao Instituto Politécnico do Porto. Em conjunto, estas instituições foram responsáveis por quase 60% da produção nacional neste período.

FIGURA 3.26: D06: DISTRIBUIÇÃO DA PRODUÇÃO CIENTÍFICA.

Número de publicações científicas com autores afiliados a instituições nacionais no domínio da Gestão de Identidade e Acesso.

Distribuição da produção científica | Por ano



Concentração de publicações científicas no domínio da Gestão de Identidade e Acesso por instituição nacional. Por exemplo, uma instituição nacional foi responsável por 44 publicações no período.

Distribuição da produção científica | Número de publicações por instituição (2017-2021)

3.7. Gestão e Governação de Segurança

O domínio de competências em cibersegurança relacionado com a *Gestão e Governação de Segurança* corresponde à governação, gestão, metodologias, processos e ferramentas destinadas à preservação da confidencialidade, integridade e disponibilidade da informação, bem como outras propriedades como autenticidade, responsabilidade e não repúdio. Do ponto de vista da atividade nacional, este domínio é um dos menos apontados pelas entidades participantes do estudo como área onde atuam. Menos de 7% das entidades indicam algum tipo de atividade neste domínio. Na maior parte (*i.e.,* 90%), as atividades são desempenhadas por equipas de, no máximo, três especialistas no domínio. Quando considerada a tipologia das atividades desempenhadas por estas entidades observa-se um destaque expressivo do *ensino superior* (*i.e.,* mais de 40% das entidades), seguido por *investigação* e por *serviços*, onde cerca de 19% indica atividade em cada uma das áreas.

Este é também o domínio de competências onde há uma maior diferença entre os resultados obtidos via questionário on-line e através do levantamento realizado através das respetivas páginas da Internet do tecido empresarial nacional. Nesta segunda vertente, o estudo revelou que cerca de 18% das empresas com atividade em cibersegurança fornecem produtos ou serviços relacionados com este domínio. Entre elas, destacam-se consultorias sobre adequação a normas técnicas, monitorização contínua e gestão e recuperação de desastres.

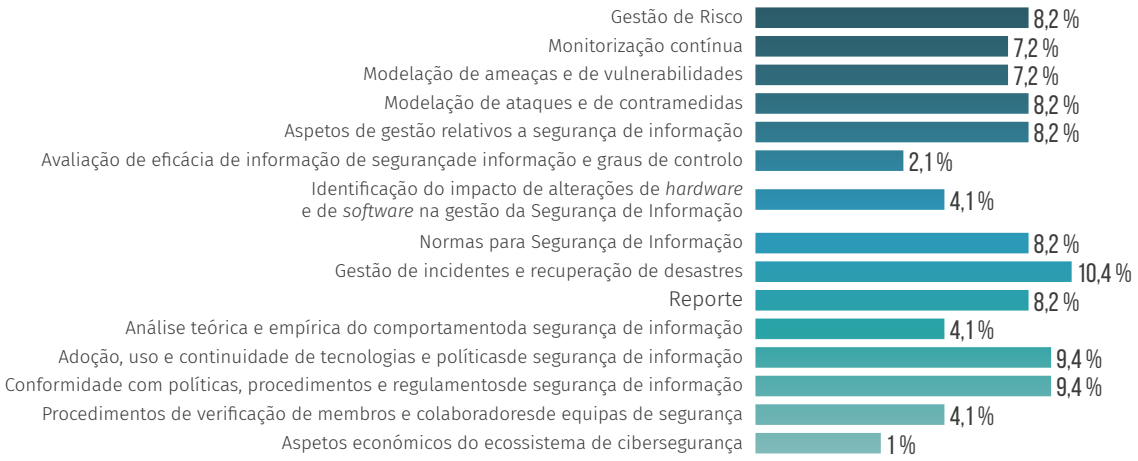
Neste ponto, é importante destacar que em entrevistas com representantes das entidades participantes no estudo foi identificada uma ambiguidade na interpretação do subdomínio *gestão de incidentes e recuperação de desastres*. Para alguns dos interlocutores, não estava claro se as atividades desempenhadas pelas suas entidades deveriam ser enquadradas neste domínio ou no domínio de competências relacionado com o *tratamento e resposta de incidentes operacionais* (*i.e.,* D04 da Tabela 1.1). Assim, parte da diferença nos resultados oriundos das duas vertentes metodológicas deste estudo podem estar relacionados com esta (pelo menos percepcionada) ambiguidade.

Um outro aspeto relevante para justificar os resultados obtidos é o número de subdomínios definidos na proposta de taxonomia europeia. A lista completa é ilustrada na Figura 3.27, na qual se observa também a distribuição das respostas dadas ao questionário on-line. Em particular, destacam-se as seguintes áreas:

- Gestão de incidentes e recuperação de desastres;
- Adoção, uso e continuidade de tecnologias e políticas de segurança de informação;
- Conformidade com políticas, procedimentos e regulamentos de segurança de informação.

FIGURA 3.27: D07: DISTRIBUIÇÃO POR SUBDOMÍNIO.

Detalhe da atuação das entidades nacionais no domínio da Gestão e Governação de Segurança no período entre 2017 e 2021.



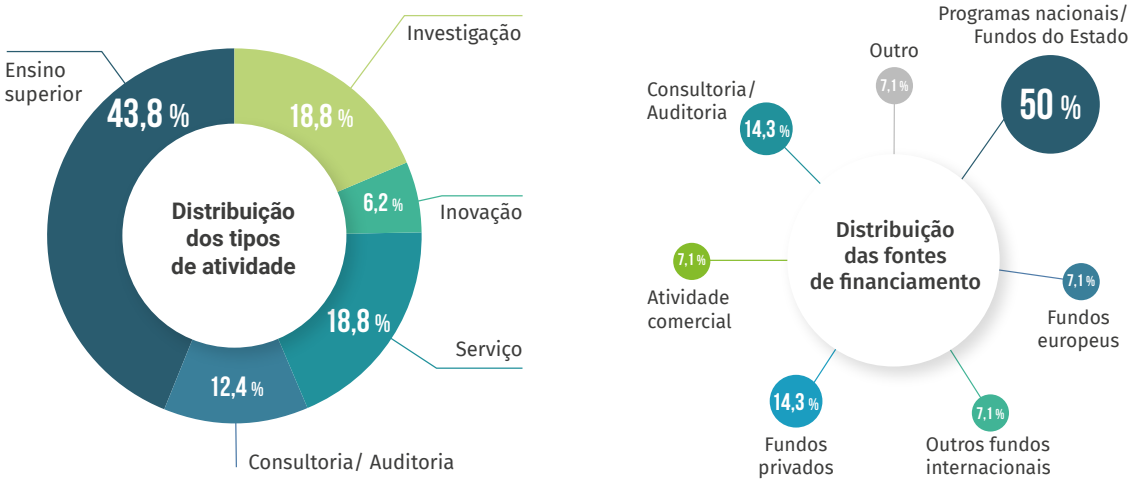
Quando consideradas as principais fontes de financiamento, tal como ilustrado na Figura 3.28, há uma concentração significativa dos *programas nacionais* ou *fundos do Estado*. Esta centralização das fontes de recursos está alinhada com a distribuição dos tipos de atividade e com o principal setor no qual tais atividades são desempenhadas, nomeadamente, o setor da *educação* (ver Figura 3.29). Aqui, ressalta-se que 20% das entidades afirmaram ter participado em *projetos nacionais* nos últimos cinco anos. Além disso,

apesar de haver entidades a apontar os *fundos europeus* como fonte de financiamento, nenhuma delas indica ter estado envolvida em projetos financiados por este tipo de fundos no mesmo período. Este é também um domínio onde não há indicações de contratos assinados com órgãos da administração pública, registo de *software* ou obtenção de registos de patente.

Já do ponto de vista das aplicações e tecnologias alvo de desenvolvimentos neste domínio de competências, destacam-se os *sistemas de informação*, as *infraestruturas críticas* e os *sistemas operativos*, sendo que este último tem particular interesse para a comunidade científica, como observado na análise das publicações científicas no domínio.

FIGURA 3.28: D07: TIPOS DE ATIVIDADE E FONTES DE FINANCIAMENTO.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio da Gestão e Governação de Segurança no período entre 2017 e 2021.



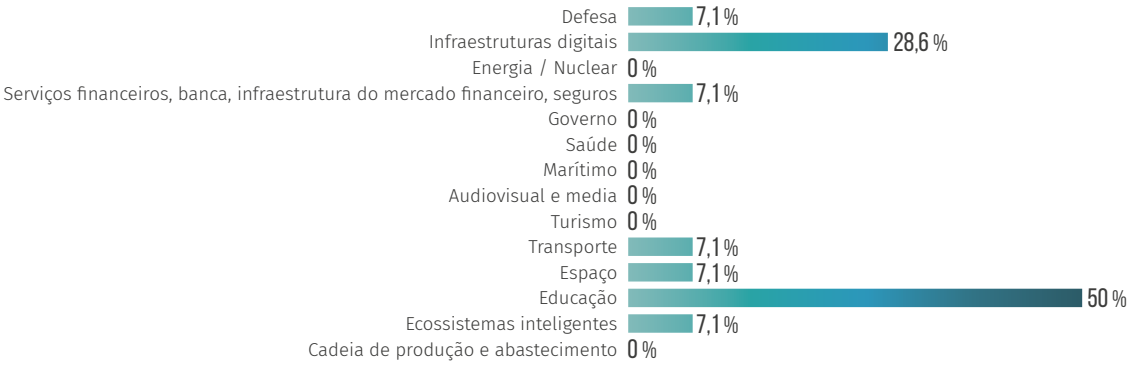
0 % Comércio | Desenvolvimento de soluções | Outro | Ensino Profissional/Certificação

0 % Produtos | Patentes | Serviços

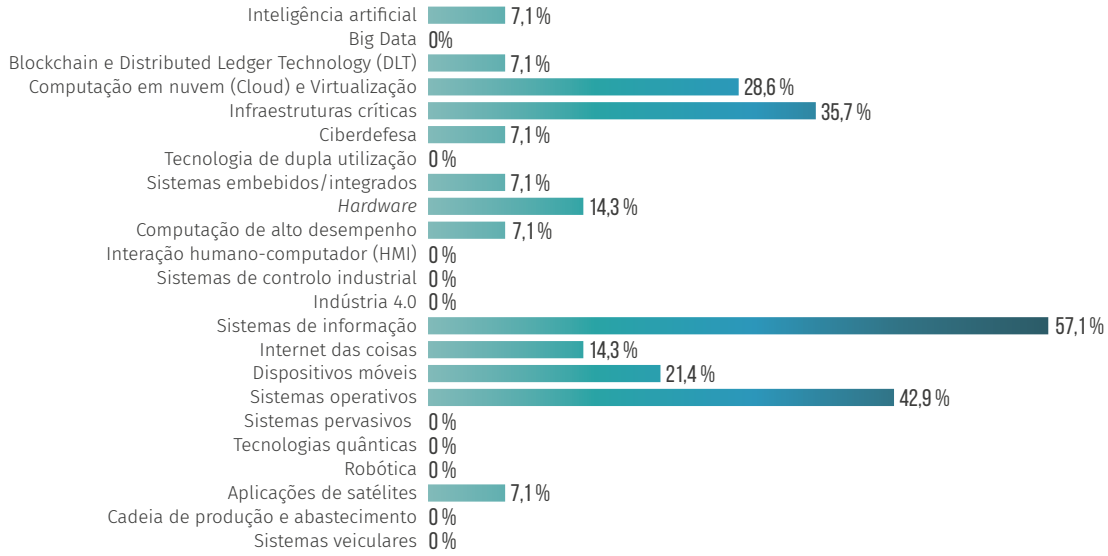
FIGURA 3.29: D07: SETORES DA ECONOMIA, APLICAÇÕES E TECNOLOGIAS.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio da Gestão e Governação de Segurança no período entre 2017 e 2021. Uma entidade pode atuar em diferentes setores da economia, áreas de aplicações e tecnologias.

Distribuição dos setores de atividade



Distribuição das aplicações e tecnologias

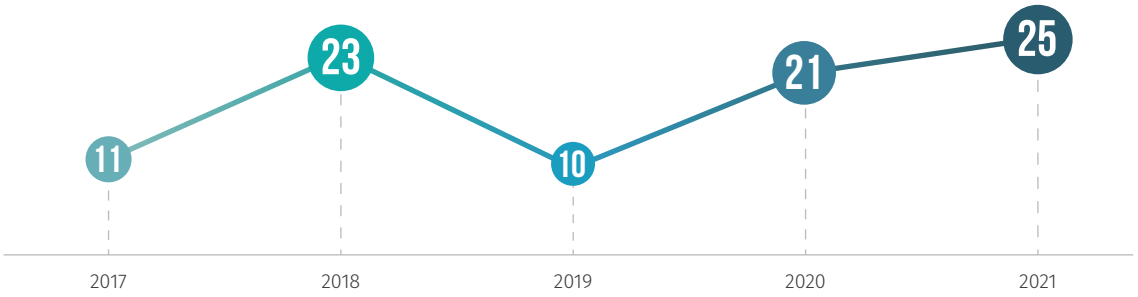


Nesta vertente, o estudo identificou um total de 90 publicações de caráter científico nos últimos cinco anos. A produção científica no domínio de competências não demonstra particular concentração, havendo pouca variação entre o número de documentos publicados pelos investigadores de cada instituição com alguma produção nesta área. Mesmo assim, e de forma a comparar com os restantes domínios, destacam-se como contribuidores neste domínio a Universidade de Lisboa, a Universidade de Coimbra e o Instituto Politécnico de Leiria.

FIGURA 3.30: D07: DISTRIBUIÇÃO DA PRODUÇÃO CIENTÍFICA.

Número de publicações científicas com autores afiliados a instituições nacionais no domínio da Gestão e Governação de Segurança.

Distribuição da produção científica | Por ano



Concentração de publicações científicas no domínio da Gestão e Governação de Segurança por instituição nacional. Por exemplo, uma instituição nacional foi responsável por 15 publicações no período.

Distribuição da produção científica | Número de publicações por instituição (2017-2021)

3.8. Rede e Sistemas Distribuídos

A segurança da informação nos domínios da rede e dos sistemas distribuídos responde pela integridade, confidencialidade, disponibilidade e não repúdio dos dados quando estes são enviados através da rede. Um sistema distribuído é um modelo no qual os componentes localizados em computadores em rede comunicam e coordenam as suas ações através da transmissão de mensagens. Neste contexto, a cibersegurança trata de todos os aspetos da computação, coordenação, integridade de mensagens, disponibilidade e confidencialidade relacionadas com este processo. A autenticação das mensagens está também no âmbito deste domínio.

De acordo com o levantamento sustentado pelo questionário on-line proposto a diferentes atores nacionais, o domínio de competências em cibersegurança aplicada às *redes de computadores* e aos *sistemas distribuídos* representa um dos mais ativos nos cinco anos analisados. Cerca de 10% das entidades participantes indicou algum tipo de atividade nesta área. Estas entidades empregam equipas de especialistas dedicados na seguinte proporção: 68% possuem equipas de um a três profissionais, 25% possuem equipas de quatro a dez profissionais, e 7% possuem equipas de 21 a 50 profissionais.

Apesar de ainda existir uma concentração nas atividades de *investigação* e de *ensino superior*, este é o domínio onde há uma maior diversidade dos desenvolvimentos em cibersegurança. Além disso, o levantamento exploratório sobre os produtos e serviços oferecidos pelo tecido empresarial nacional identificou que cerca de 20% das 120 empresas têm competências de cibersegurança em redes ou sistemas distribuídos. Este é o domínio com maior concentração de atividade nesta vertente do estudo, que é idêntico ao domínio relacionado com a *Engenharia de Segurança de Software e de Hardware* (*i.e.*, D09).

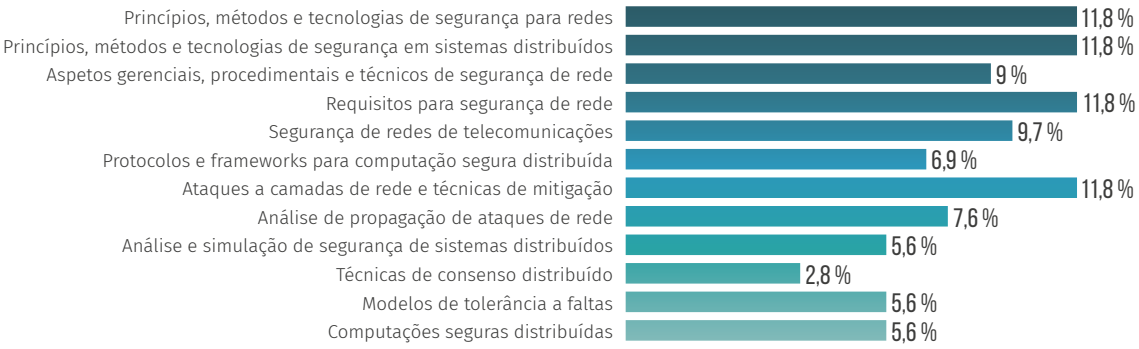
Como observado na Figura 3.32, para todas as tipologias de atividade consideradas neste estudo, pelo menos, 11% das entidades indicou algum tipo de atuação. Esta heterogeneidade é também refletida nas fontes principais de financiamento das atividades no domínio. Os programas nacionais lideram o financiamento através de programas de investigação (indicado por 40% das entidades), programas de inovação (indicado por 15% das entidades) e contratos com a administração pública (indicado por 5% das entidades). De seguida, os fundos europeus financiaram a atividade de cibersegurança em redes e sistemas distribuídos de aproximadamente 40% das entidades participantes do estudo.

Do ponto de vista dos subdomínios da taxonomia da ENISA, observa-se também uma atuação diversificada e volumosa, com particular destaque nos seguintes tópicos:

- Princípios, métodos e tecnologias de segurança para redes;
- Princípios, métodos e tecnologias de segurança em sistemas distribuídos;
- Requisitos para segurança de rede;
- Ataques às camadas de redes e técnicas de mitigação.

FIGURA 3.31: D08: DISTRIBUIÇÃO POR SUBDOMÍNIO.

Detalhe da atuação das entidades nacionais no domínio de Redes e Sistemas Distribuídos no período entre 2017 e 2021.



Os principais setores da economia para os quais a atividade nacional está orientada incluem as *infraestruturas digitais*, a *educação*, o *governo* e *saúde*. A maioria das entidades participantes indicam desenvolvimentos ligados aos *sistemas de informação*, *internet das coisas* e *infraestruturas críticas*. Apesar de existir um grande interesse global nas tecnologias relacionadas com a *computação em nuvem* e *virtualização*, o estudo demonstrou que estas apenas se destacam neste domínio de competências (ver Figura 3.33).

Apesar de nenhuma das entidades participantes do estudo ter indicado a obtenção de registos de patentes no período, o levantamento feito no WIPO revelou duas patentes concedidas a inventores ligados a uma instituição nacional. Em particular, as patentes estão ligadas a métodos de transmissão segura de dados em ambientes sem fios e foram desenvolvidas por investigadores de um centro de investigação (*i.e.*, o Instituto de Telecomunicações da Universidade de Aveiro).

FIGURA 3.32: D08: TIPOS DE ATIVIDADE E FONTES DE FINANCIAMENTO.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio de Redes e Sistemas Distribuídos no período entre 2017 e 2021.

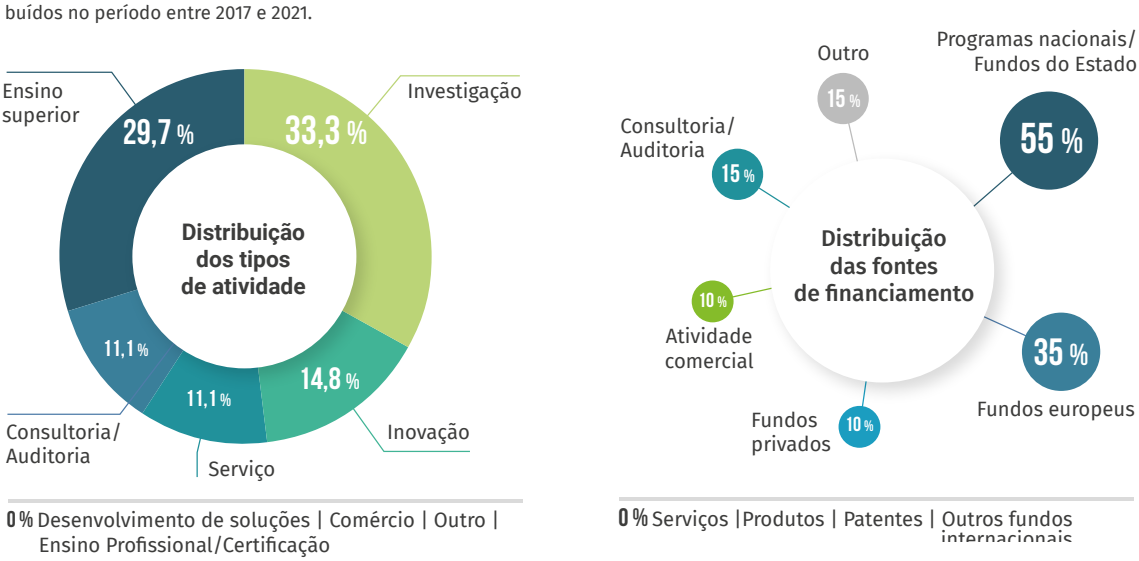
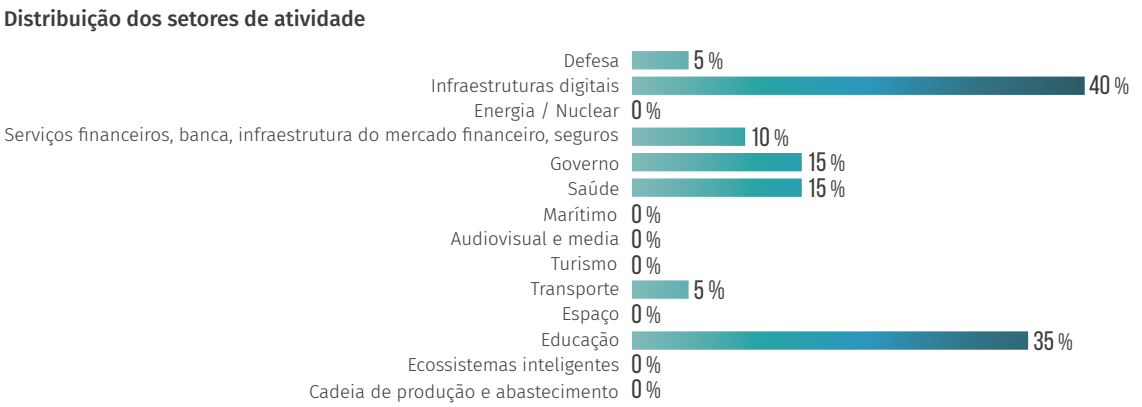
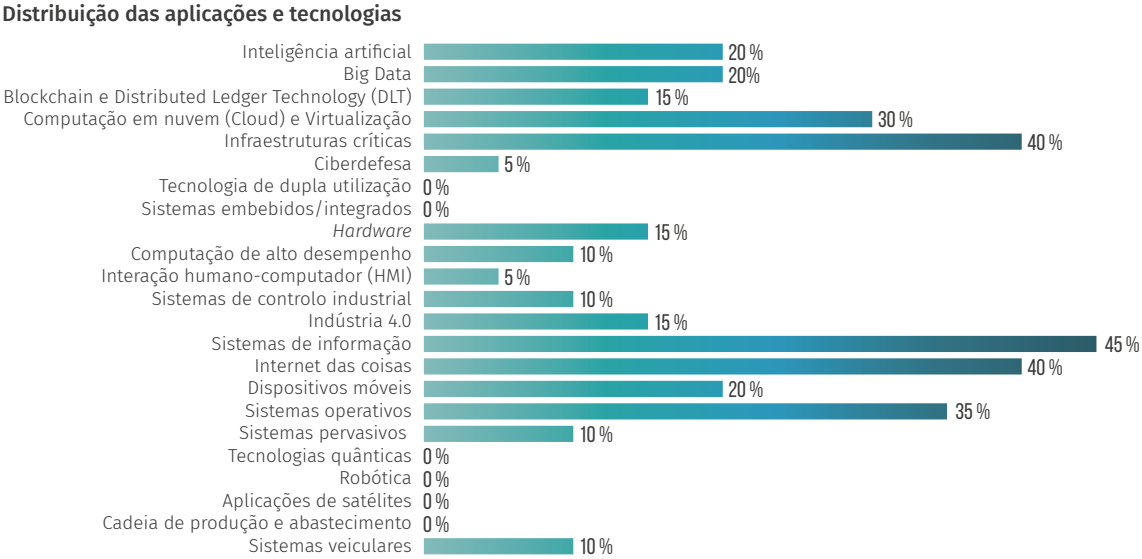


FIGURA 3.33: D08: SETORES DA ECONOMIA, APLICAÇÕES E TECNOLOGIAS.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio de Redes e Sistemas Distribuídos no período entre 2017 e 2021. Uma entidade pode atuar em diferentes setores da economia, áreas de aplicações e tecnologias.



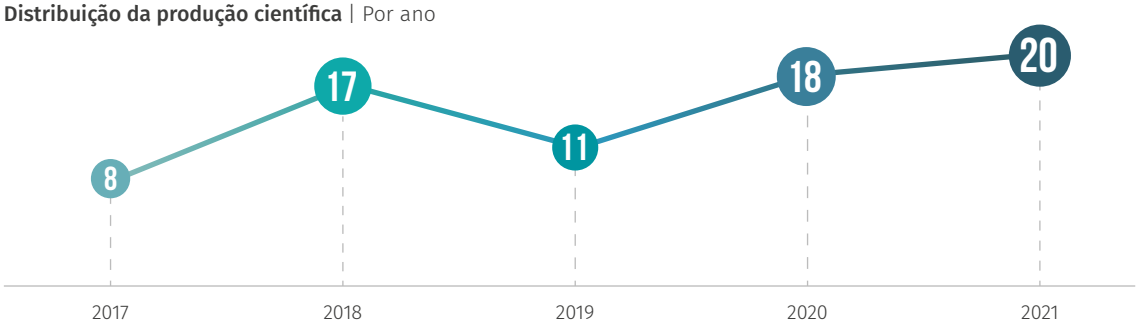


A comunidade nacional também demonstra regularidade na produção de publicações de caráter científico no domínio de competências de cibersegurança em redes e em sistemas distribuídos. Ao longo dos últimos cinco anos, investigadores ligados a 24 instituições nacionais distintas foram responsáveis por 74 publicações (ver Figura 3.34). Este é o domínio com o segundo maior número de instituições diferentes a produzir trabalho na forma de publicações, ficando atrás apenas do domínio de competências em *Engenharia de Segurança de Software e de Hardware* (*i.e.,* D09, descrito na Secção 3.9). Entre elas, destacam-se a Universidade de Coimbra, a Universidade do Porto e a Universidade de Lisboa. Na Figura 3.34, é possível constatar também que, nos últimos três anos, tem havido um pequeno, mas constante, aumento do volume de produção científica neste domínio.

FIGURA 3.34: D08: DISTRIBUIÇÃO DA PRODUÇÃO CIENTÍFICA.

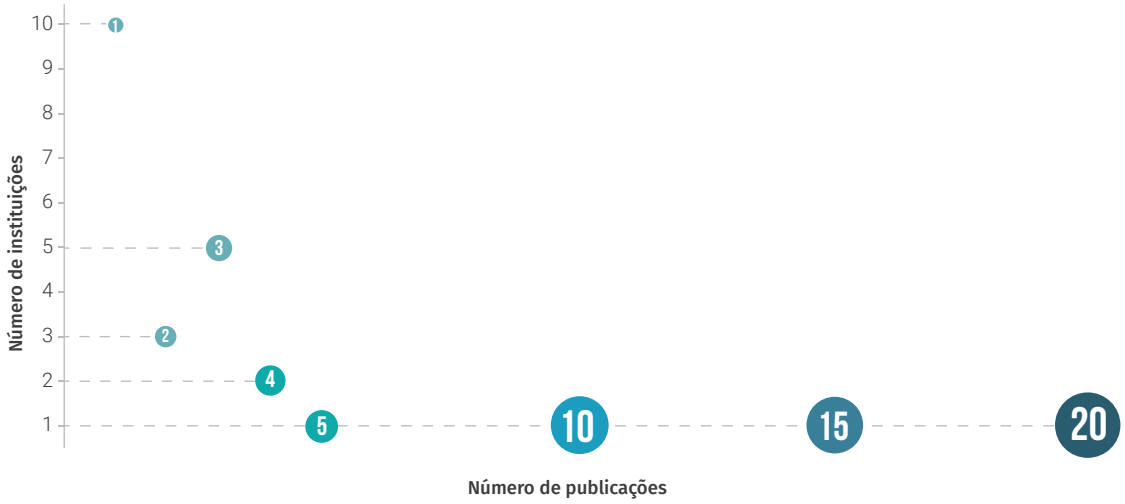
Número de publicações científicas com autores afiliados a instituições nacionais no domínio de Redes e Sistemas Distribuídos.

Distribuição da produção científica | Por ano



Concentração de publicações científicas no domínio de Redes e Sistemas Distribuídos por instituição nacional. Por exemplo, uma instituição nacional foi responsável por 20 publicações no período.

Distribuição da produção científica | Número de publicações por instituição (2017-2021)



3.9. Engenharia de Segurança de *Software* e de *Hardware*

Aspetos de segurança no ciclo de vida do desenvolvimento de *software* e *hardware*, tais como análise de risco e requisitos, conceção de arquitetura, implementação de código, validação, verificação, teste, implementação e monitorização do funcionamento em tempo de execução são as competências centrais no domínio da cibersegurança aplicada ao desenvolvimento de *Software* e *Hardware*.

Em relação ao número de entidades com equipas dedicadas a desenvolvimentos em cibersegurança, o domínio de competências em *Engenharia de Segurança de Software e de Hardware* é o segundo mais apontado pelas empresas participantes do estudo. Mais de 10% dos interlocutores indicou esta área nas respostas ao questionário on-line. Estas equipas são formadas por até três profissionais em 62% das entidades. Em 31% delas, as equipas possuem de quatro a dez profissionais e, em 7% das entidades, as equipas empregam entre 11 e 20 especialistas.

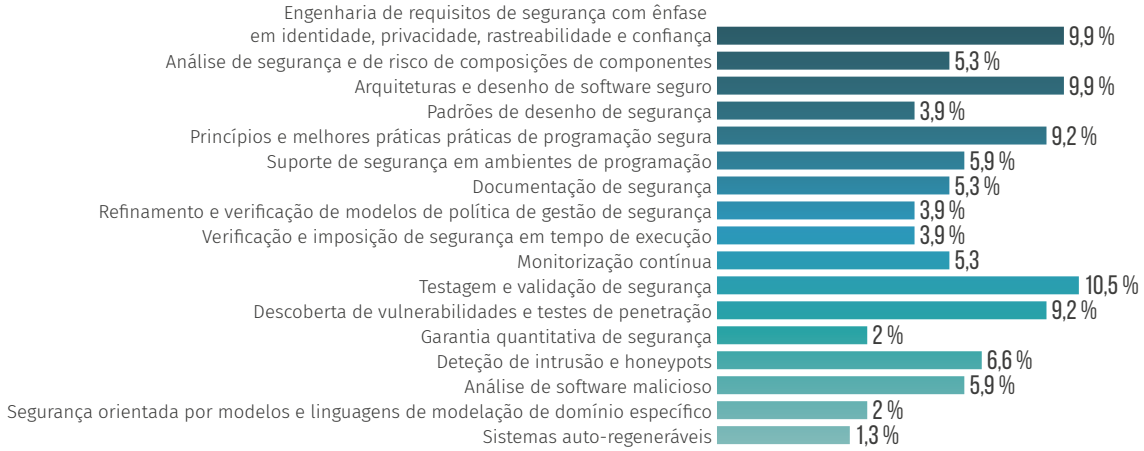
Tal como mencionado na Secção 3.8, além deste domínio ser o que tem maior número de empresas a listar publicamente competências (20% das 120 com atuação em cibersegurança), o levantamento exploratório sobre os associados coletivos das entidades listadas na Tabela 2.1 revelou, também, grande variedade de produtos e serviços relacionados. Mais especificamente, este é o domínio com a maior diversidade de atuação do tecido empresarial nacional. Importa ressaltar que diversas empresas anunciam serviços de teste de penetração e deteção de intrusão.

A Figura 3.36 mostra que as atividades ligadas à *inovação* e ao *ensino superior* ainda são predominantes entre as entidades que responderam ao questionário on-line. Contudo, as áreas de *inovação*, *serviços* e *consultoria/auditoria* aparecem também destacadas e são confirmadas pela vertente de levantamento exploratório de dados públicos.

Quando analisadas as principais fontes de financiamento das atividades neste domínio, destacam-se os fundos nacionais e europeus, responsáveis por financiar mais de 30% das entidades via projetos europeus, 35% via projetos nacionais e 40% via projetos de inovação. Além disso, 20% das entidades afirmou ter estabelecido contratos com a indústria nos últimos cinco anos. Neste domínio, destacam-se também os fundos privados e a atividade comercial. Apesar da existência de indicações sobre o registo de *software* e patente, nenhuma entidade aponta a exploração de direitos de propriedade intelectual como fonte de financiamento das suas atividades.

FIGURA 3.35: D09: DISTRIBUIÇÃO POR SUBDOMÍNIO.

Detalhe da atuação das entidades nacionais no domínio da Engenharia de Segurança de *Software* e de *Hardware* no período entre 2017 e 2021.



Tendo em conta a distribuição das atividades entre os subdomínios de competências definidos pela ENISA, em Portugal destacam-se entidades a atuar em:

- Testes e validação de segurança;
- Engenharia de requisitos de segurança com ênfase em identidade, privacidade, rastreabilidade e confiança;
- Arquiteturas e desenho de *software* seguro;
- Descoberta de vulnerabilidades e testes de penetração.

Outro foco de ambiguidade observado pelos intervenientes das entidades participantes é o subdomínio *engenharia de requisitos de segurança com ênfase em identidade, privacidade, rastreabilidade e confiança*, que, em alguns casos, foi interpretado e, consequentemente, apontado como uma atividade do domínio da *Gestão de Identidade e Acesso* (ver Secção 3.6).

Ainda de acordo com as respostas ao questionário on-line, este domínio de competências confirma o interesse nacional, observado em todos os outros domínios nos setores das *infraestruturas digitais* e da *educação*. Combinados, estes setores são objeto de desenvolvimentos por mais de 40% das entidades participantes no estudo. Além dos setores governamentais e da saúde, aparece, pela primeira vez, como destaque, a área que engloba os *serviços financeiros, banca, infraestruturas do mercado financeiro e seguros*. Quanto às aplicações e tecnologias, aparece também como destaque, pela primeira vez, a *inteligência artificial* e *big data*.

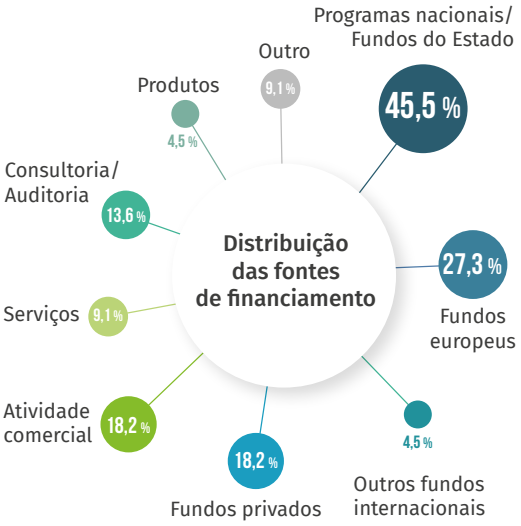
Tal como inicialmente descrito na Secção 2.2, o domínio de competências em cibersegurança ligado a *Engenharia de Segurança de Software e de Hardware* é responsável pelo maior volume de publicações científicas ao longo dos cinco anos considerados no estudo. Este é também o domínio onde há um maior número de instituições nacionais a produzir resultados neste formato. Mais especificamente, investigadores ligados a 33 instituições nacionais foram responsáveis por 335 publicações de caráter científico no período considerado neste estudo. Em comparação com os anos com maior e menor volume de publicações, observa-se uma duplicação no volume de trabalhos, nomeadamente, 40 publicações em 2017 e 102 publicações em 2021 (ver evolução na Figura 3.38).

Assim, como observado no domínio da cibersegurança na *Gestão de Identidade e Acesso*, o maior volume de instituições a explorar a área e a multidisciplinaridade dos temas onde os investigadores têm direcionado esforços são as principais razões para a grande concentração de publicações neste domínio de competências.

FIGURA 3.36: D09: TIPOS DE ATIVIDADE E FONTES DE FINANCIAMENTO.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio da Engenharia de Segurança de *Software* e de *Hardware* no período entre 2017 e 2021.

0 % Comércio | Ensino profissional/Certificação | Outro

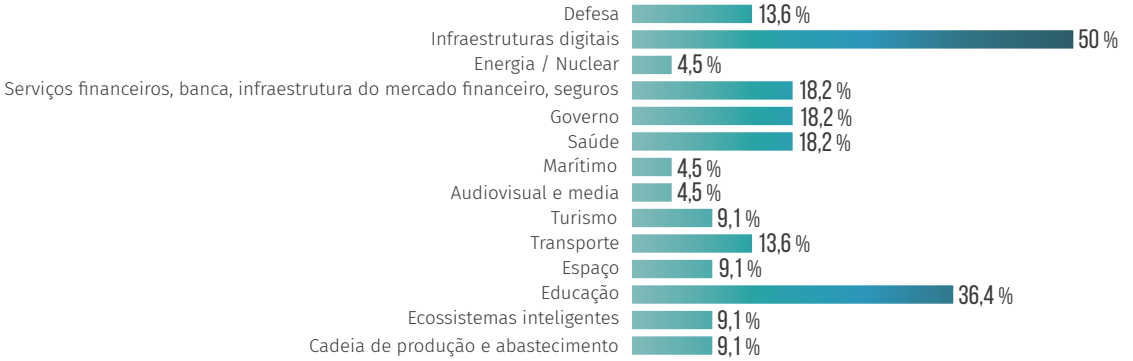


0 % Patentes

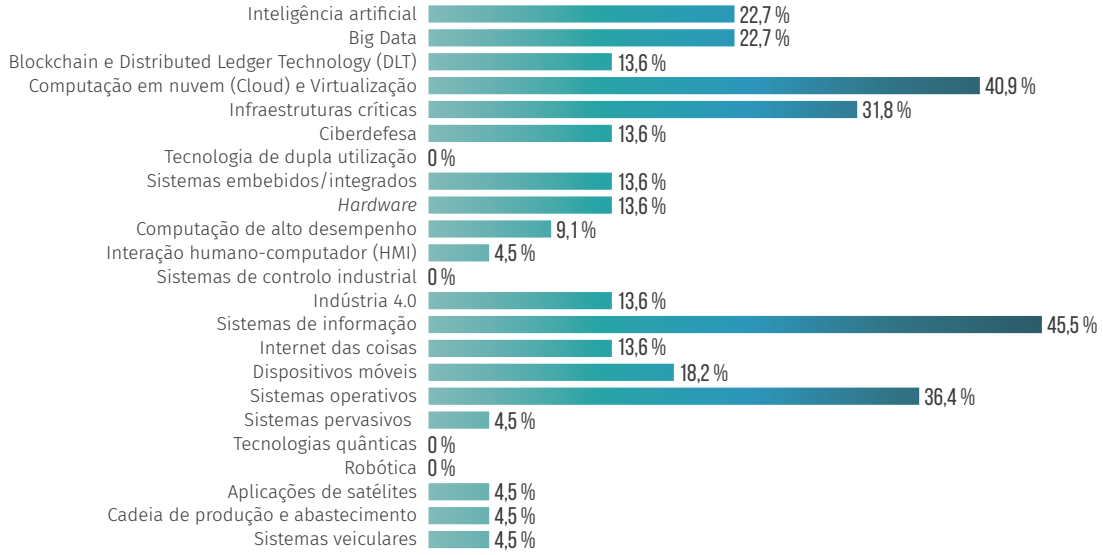
FIGURA 3.37: D09: SETORES DA ECONOMIA, APLICAÇÕES E TECNOLOGIAS.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio da Engenharia de Segurança de *Software* e de *Hardware* no período entre 2017 e 2021. Uma entidade pode atuar em diferentes setores da economia, áreas de aplicações e tecnologias.

Distribuição dos setores de atividade



Distribuição das aplicações e tecnologias

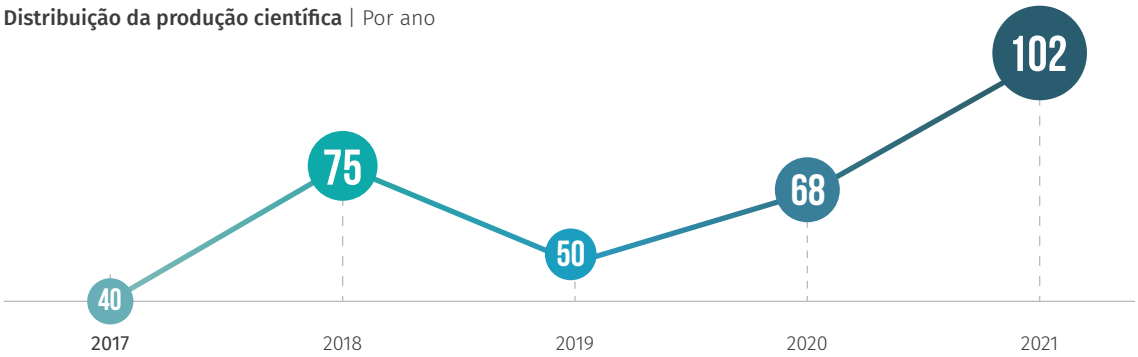


Já do ponto de vista da concentração da produção entre as instituições a promover a área, observa-se grande destaque da Universidade de Coimbra, seguida pela Universidade do Porto, Universidade de Lisboa, Universidade de Aveiro e Universidade do Minho. Esta dimensão do estudo é ilustrada na Figura 3.38.

FIGURA 3.38: D09: DISTRIBUIÇÃO DA PRODUÇÃO CIENTÍFICA.

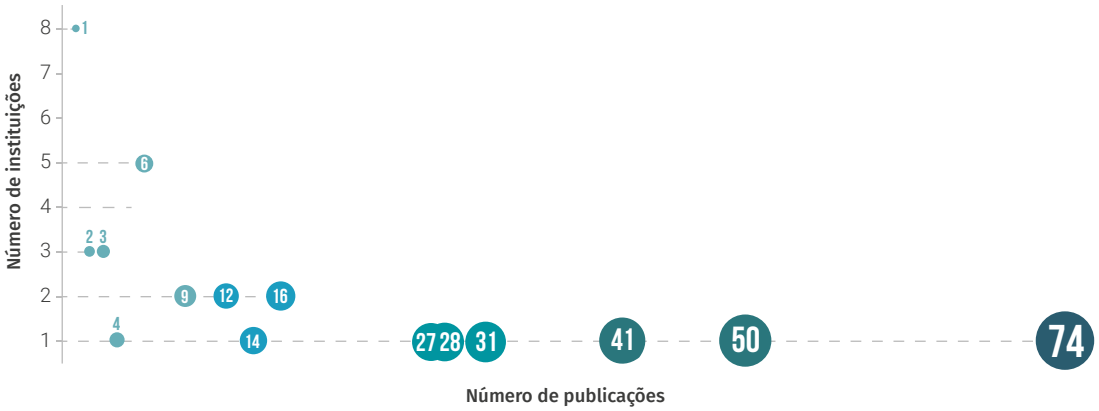
Número de publicações científicas com autores afiliados a instituições nacionais no domínio da Engenharia de Segurança de *Software* e de *Hardware*.

Distribuição da produção científica | Por ano



Concentração de publicações científicas no domínio da Engenharia de Segurança de *Software* e de *Hardware* por instituição nacional. Por exemplo, uma instituição nacional foi responsável por 74 publicações no período.

Distribuição da produção científica | Número de publicações por instituição (2017-2021)



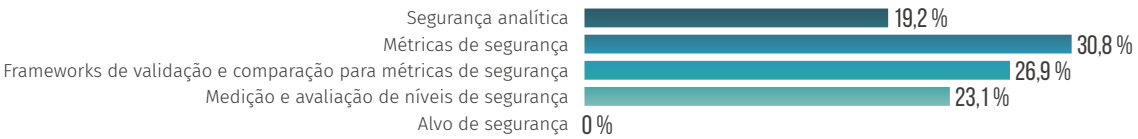
3.10. Medidas de Segurança

O domínio de competências relacionado com *Medidas de Segurança* envolve os conhecimentos e ferramentas utilizadas para facilitar a tomada de decisões e melhorar o desempenho e a responsabilização através da recolha, análise e comunicação de dados relevantes relacionados com o desempenho da cibersegurança. O objetivo de medir o desempenho passa por monitorizar o estado das atividades medidas e facilitar a melhoria dessas atividades através da aplicação de ações corretivas baseadas nas medidas observadas.

Relativamente ao cenário nacional, este domínio corresponde a um dos grupos com menor número de entidades a apontar algum tipo de atividade. Pouco mais de 6% dos participantes no estudo, via questionário on-line, indicou que as suas instituições possuem equipas dedicadas ao tema, proporção semelhante à observação via análise exploratória dos produtos e serviços oferecidos pelo tecido empresarial nacional. As respostas ao questionário vieram, maioritariamente, de instituições do ensino superior, centros de investigação, consultoras e empresas dedicadas ao setor dos serviços que empregam, em 90% dos casos, equipas de até três especialistas no domínio. Esta distribuição é também refletida nos tipos de atividade a que se dedicam. Tal como apresentado na Figura 3.40, destacam-se a *investigação*, *ensino superior*, *inovação* e a comercialização *serviços* em cibersegurança.

FIGURA 3.39: D10: DISTRIBUIÇÃO POR SUBDOMÍNIO.

Detalhe da atuação das entidades nacionais no domínio das Medidas de Segurança no período entre 2017 e 2021.



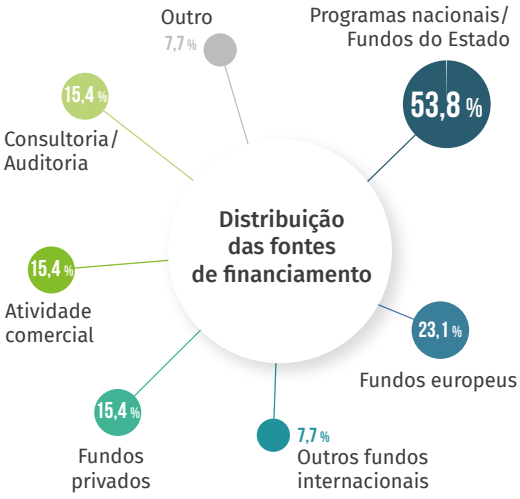
Quando analisadas as principais fontes de financiamento das atividades neste domínio, constata-se que os programas nacionais e os fundos europeus são responsáveis por mais de 55% do volume investido. Tal investimento concentra-se, principalmente, em projetos nacionais, responsável por financiar 40% das entidades participantes em projetos europeus e em projetos de inovação, com cerca de 20% de entidades financiadas por cada tipologia de projeto. Além disso, cerca de 30% das entidades indicaram ter assinado contratos com a indústria nos últimos cinco anos.

Assim como observado na maioria dos domínios de competências, os setores ligados às *infraestruturas digitais* e à *educação* concentram o maior volume dos desenvolvimentos nacionais. Apesar do relativo baixo interesse nacional neste domínio, parte dos trabalhos estão direcionados para aplicações e tecnologias em franco desenvolvimento global, por exemplo, a *computação em nuvem* e as tecnologias de *virtualização*. A distribuição das respostas relativas a esta vertente do estudo é apresentada na Figura 3.40. Já do ponto de vista dos subdomínios da taxonomia da ENISA, o interesse das entidades nacionais está homogeneamente distribuído, com algum destaque para as *Medidas de Segurança* e para as *frameworks para validação e comparação de métricas de segurança* (ver Figura 3.39).

FIGURA 3.40: D10: TIPOS DE ATIVIDADE E FONTES DE FINANCIAMENTO.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio das Medidas de Segurança no período entre 2017 e 2021.

0 % Comércio | Outro

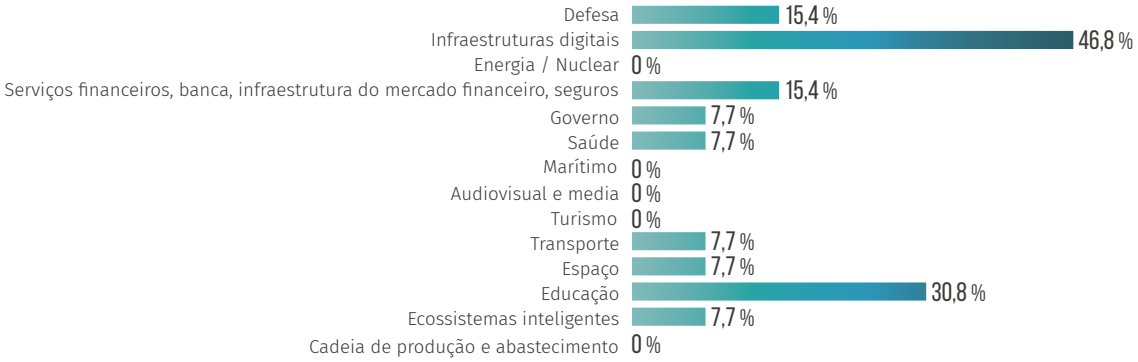


0 % Produtos | Patentes | Serviços

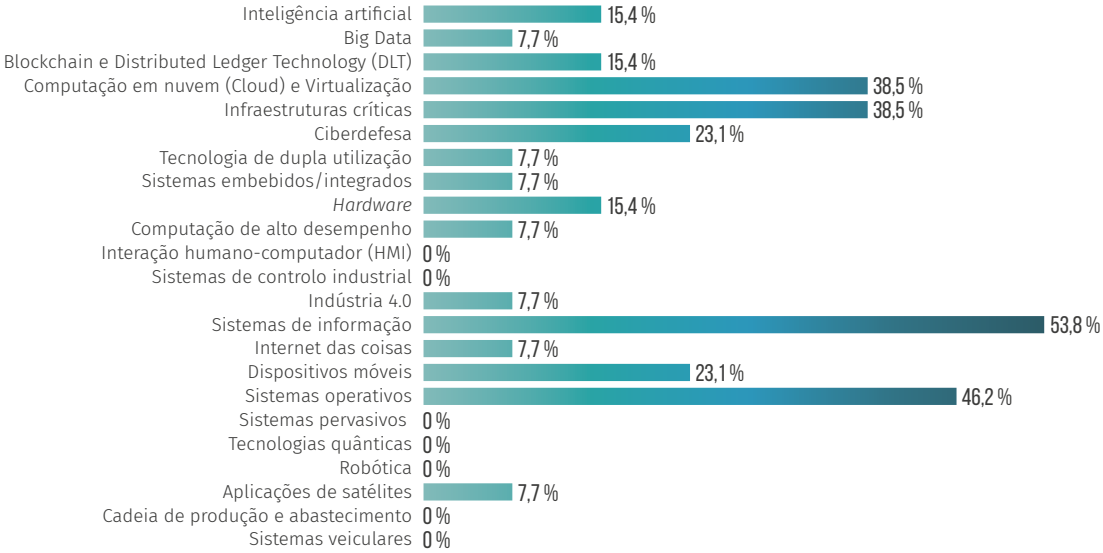
FIGURA 3.41: D10: SETORES DA ECONOMIA, APLICAÇÕES E TECNOLOGIAS.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio das Medidas de Segurança no período entre 2017 e 2021. Uma entidade pode atuar em diferentes setores da economia, áreas de aplicações e tecnologias.

Distribuição dos setores de atividade



Distribuição das aplicações e tecnologias

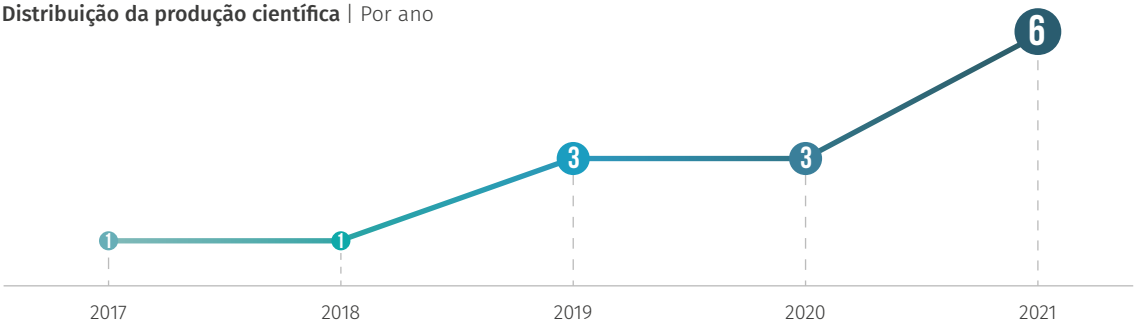


A menor atividade nacional neste domínio de competências é também refletida no resultado do levantamento das publicações científicas de autoria de investigadores afiliados a instituições nacionais. No total, foram identificadas apenas 14 publicações nos últimos cinco anos, o menor volume entre os domínios analisados. Além disso, um total de dez instituições nacionais estiveram envolvidas nestas publicações, o que acaba por representar uma menor concentração no número de publicações por instituição (ver Figura 3.42). Ainda que relativo, os destaques neste domínio são a Universidade de Coimbra e a Universidade do Porto.

FIGURA 3.42: D10: DISTRIBUIÇÃO DA PRODUÇÃO CIENTÍFICA.

Número de publicações científicas com autores afiliados a instituições nacionais no domínio das Medidas de Segurança.

Distribuição da produção científica | Por ano



Concentração de publicações científicas no domínio das Medidas de Segurança por instituição nacional. Por exemplo, uma instituição nacional foi responsável por cinco publicações no período.

Distribuição da produção científica | Número de publicações por instituição (2017-2021)

3.11. Tecnologia e Aspetos Legais

De acordo com a definição da taxonomia europeia, o domínio de competências em cibersegurança que relaciona *Tecnologia e Aspetos Legais* refere-se às questões relacionadas com o uso indevido da tecnologia, distribuição e/ou reprodução ilícita de material abrangido pelos direitos de propriedade intelectual e a aplicação da lei relacionada com a cibercriminalidade e os direitos digitais.

Tendo em conta o resultado do questionário on-line, cerca de 8% das entidades participantes afirmam desenvolver algum tipo de atividade neste domínio. Tal como ilustrado na Figura 3.44, essa atividade está amplamente concentrada no *ensino superior* e na *inovação*. A prestação de serviços também se destaca com, aproximadamente, 17% das entidades indicando atividades deste tipo. Além disso, em 81% dos casos, as entidades empregam equipas de especialistas dedicados às atividades do domínio com, no máximo, três profissionais. Para os restantes 19%, as equipas são compostas por entre quatro e dez funcionários.

Já o resultado do levantamento exploratório ao tecido empresarial identificou que 5% das entidades com atividade em cibersegurança oferecem serviços especializados neste domínio de competências. A maior parte delas divulga serviços de assessoria jurídica para a implementação de mecanismos relacionados com o RGPD. Questões legais ligadas às respostas a incidentes de segurança também aparecem listadas.

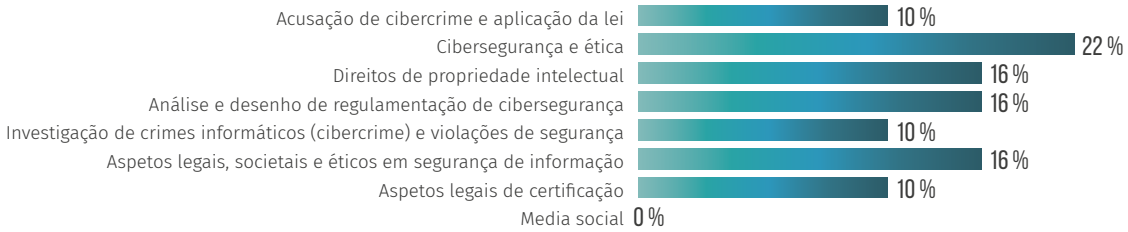
Para estas entidades, o financiamento das atividades relacionadas com os aspetos legais do uso da tecnologia é, maioritariamente, oriundo de programas nacionais e fundos do Estado. Em particular, através de acordos com órgãos do governo (indicado por 20% das entidades) e de contratos com a indústria (indicado por mais de 20% das entidades). Além disso, cerca de 20% dos interlocutores afirmaram que as suas instituições financiam atividades nesta área através de fundos próprios.

Ao classificar a atividade nacional entre os subdomínios da taxonomia europeia (ver distribuição total na Figura 3.43), observa-se uma ligeira concentração em:

- Cibersegurança e ética:
- Direito de propriedade intelectual;
- Análise de desempenho de regulamentação de cibersegurança;
- Aspetos legais de certificação.

FIGURA 3.43: D11: DISTRIBUIÇÃO POR SUBDOMÍNIO.

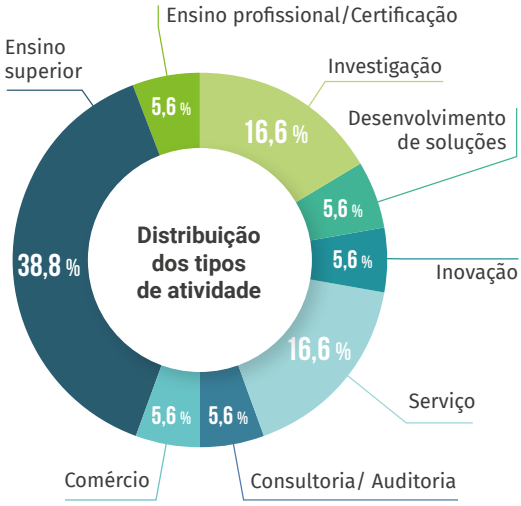
Detalhe da atuação das entidades nacionais no domínio de Tecnologia e Aspetos Legais no período entre 2017 e 2021.



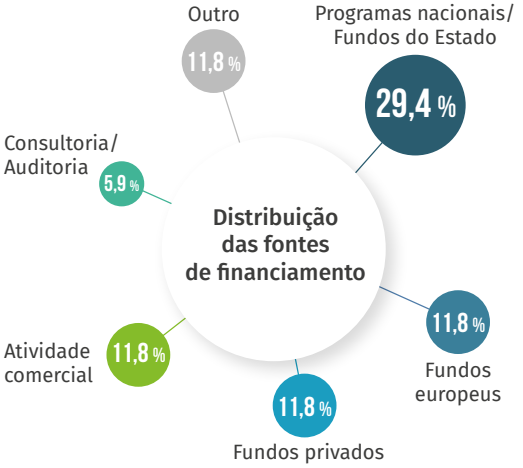
É interessante notar que nenhuma entidade apontou o subdomínio que envolve a *media social* como área de interesse ou atuação. Além disso, de acordo com o resultado do questionário on-line, observa-se uma significativa concentração de trabalho efetuado no setor da *educação*, seguido pelas *infraestruturas digitais*. A maioria dos desenvolvimentos têm como contexto de aplicação os *sistemas de informação* e os *sistemas operativos*.

FIGURA 3.44: D11: TIPOS DE ATIVIDADE E FONTES DE FINANCIAMENTO.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio de Tecnologia e Aspetos Legais no período entre 2017 e 2021.



0 % Outro

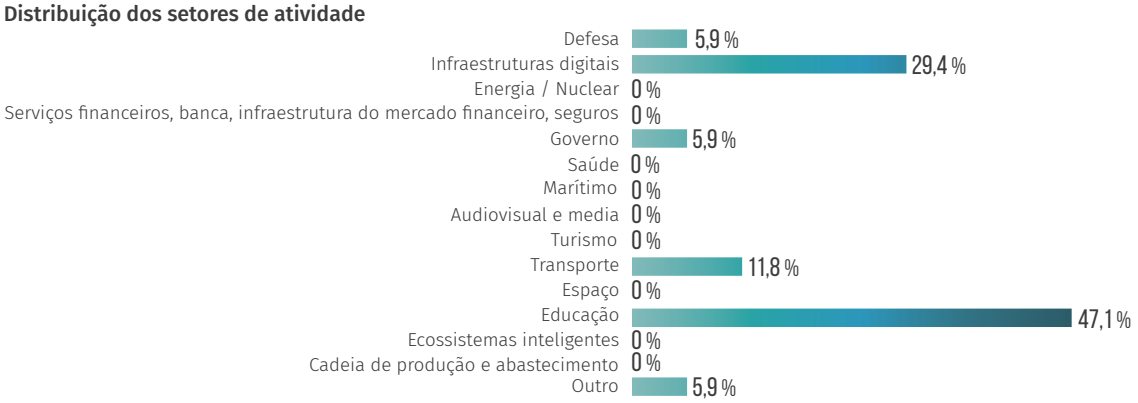


0 % Produtos | Patentes | Serviços | Outros fundos internacionais

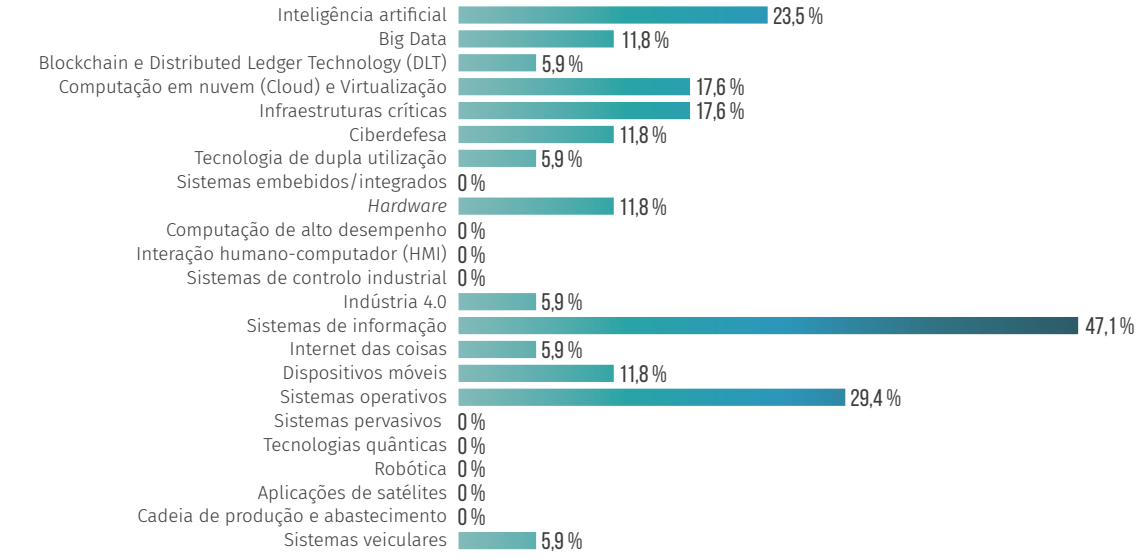
FIGURA 3.45: D11: SETORES DA ECONOMIA, APLICAÇÕES E TECNOLOGIAS.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio de Tecnologia e Aspetos Legais no período entre 2017 e 2021. Uma entidade pode atuar em diferentes setores da economia, áreas de aplicações e tecnologias.

Distribuição dos setores de atividade



Distribuição das aplicações e tecnologias

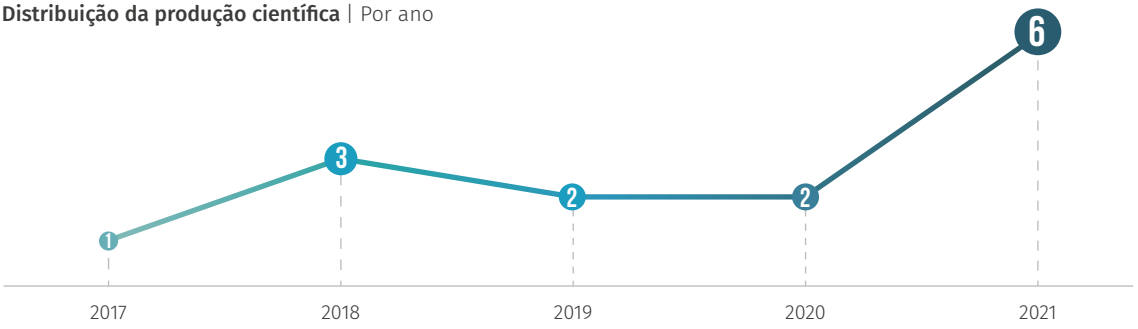


Apesar da forte concentração de atividades no setor da educação, em particular, por instituições do ensino superior, este domínio de competências não se destaca na produção de trabalhos científicos. De acordo com o levantamento feito em repositórios públicos, investigadores ligados a 13 instituições nacionais foram responsáveis por 14 publicações de caráter científico nos últimos cinco anos. Como pode ser observado na Figura 3.46, não há particular concentração de publicações por nenhuma das instituições identificadas no estudo.

FIGURA 3.46: D11: DISTRIBUIÇÃO DA PRODUÇÃO CIENTÍFICA.

Número de publicações científicas com autores afiliados a instituições nacionais no domínio de Tecnologia e Aspetos Legais.

Distribuição da produção científica | Por ano



Concentração de publicações científicas no domínio de Tecnologia e Aspetos Legais por instituição nacional. Por exemplo, uma instituição nacional foi responsável por duas publicações no período.

Distribuição da produção científica | Número de publicações por instituição (2017-2021)

3.12. Fundamentos Teóricos da Análise e de Desenho de Segurança

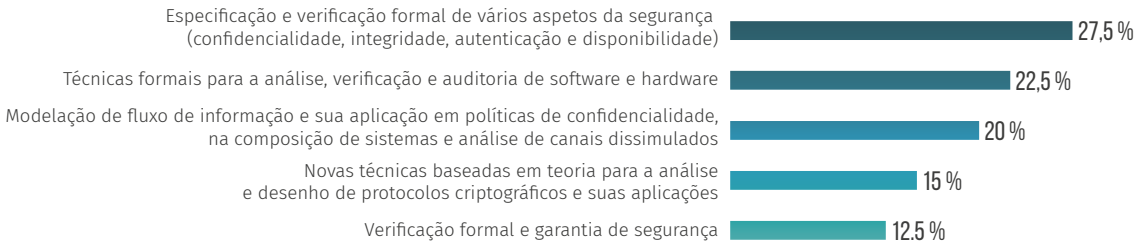
O domínio de competências que engloba os *Fundamentos teóricos da análise e do desenho de segurança* refere-se à utilização de técnicas de análise e verificação baseadas em métodos formais para fornecer provas teóricas das propriedades de segurança em *software*, *hardware* e na conceção de algoritmos. Este domínio foi apontado por, aproximadamente, 6% dos participantes do estudo como objeto de atividades e desenvolvimento. As atividades principais correspondem ao *ensino superior* e à *investigação* e contam com equipas de, no máximo, três especialistas em 80% das entidades. As restantes, empregam equipas de quatro a dez profissionais especializados.

As características académico-científicas deste domínio de competências são refletidas na quase inexistente oferta de produtos e serviços relacionados pelo tecido empresarial nacional. De acordo com a vertente do estudo que explorou estas entidades, apenas uma empresa lista competências em Investigação e Desenvolvimento (I&D) de aspetos teóricos e fundamentais da cibersegurança.

Como ilustrado na Figura 3.48, a principal fonte de financiamento das atividades reportadas via questionário on-line são os *programas nacionais* e os *fundos do Estado*. Estas linhas financiaram 20% dos participantes via projetos nacionais, 10% via projetos de inovação e 20% via contratos diretos com instituições governamentais. Entretanto, uma fonte de financiamento que se destaca apenas neste domínio são os *fundos privados*. Se considerados em conjunto com as fontes próprias (i.e., opção *outros* na Figura 3.48), o capital privado assume o papel principal no financiamento de atividades. Este é o único domínio onde esta dinâmica é identificada. Além disso, a atividade de *consultoria* e *auditoria* técnica também se destacam neste domínio.

FIGURA 3.47: D12: DISTRIBUIÇÃO POR SUBDOMÍNIO.

Detalhe da atuação das entidades nacionais no domínio dos Fundamentos Teóricos da Análise e de Desenho de Segurança no período entre 2017 e 2021.



Do ponto de vista da distribuição das atividades entre as subáreas do domínio, a Figura 3.47 mostra que as entidades participantes no estudo possuem atuação abrangente. Entretanto, destacam-se as áreas da *especificação e verificação formal de vários aspetos da segurança* e das *técnicas formais para a análise, verificação e auditoria de software e hardware*. Os setores com maior concentração de atividades são a *educação* e as *infraestruturas digitais*. Além disso, dois outros setores têm destaque, principalmente, quando comparados com as distribuições dos restantes domínios. Estes setores correspondem aos serviços financeiros (*i.e., serviços financeiros, banca, infraestrutura do mercado financeiro e seguros*) e aos serviços de *audiovisual e media*.

Ao avaliar as aplicações e tecnologias envolvidas nos desenvolvimentos nacionais, além dos *sistemas de informação* e dos *sistemas operativos*, que são centrais em todos os domínios deste estudo, há, pela primeira vez, destaque para as tecnologias ligadas à *ciberdefesa*, *aplicações de satélites* e *computação de alto desempenho*. O panorama global desta vertente é apresentado na Figura 3.49.

FIGURA 3.48: D12: TIPOS DE ATIVIDADE E FONTES DE FINANCIAMENTO.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio dos Fundamentos Teóricos da Análise e de Desenho de Segurança no período entre 2017 e 2021.

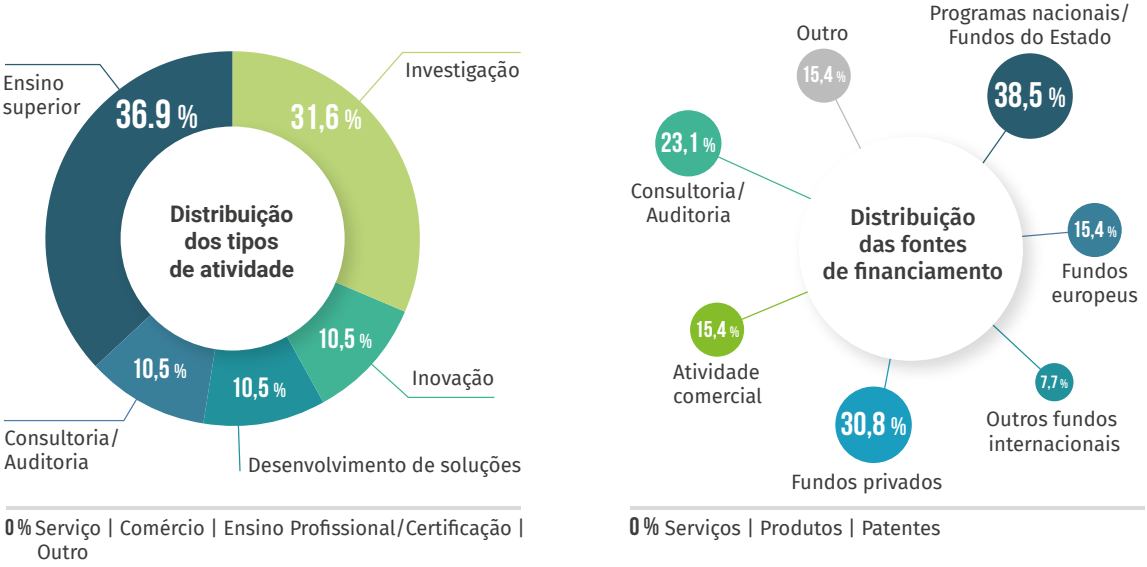
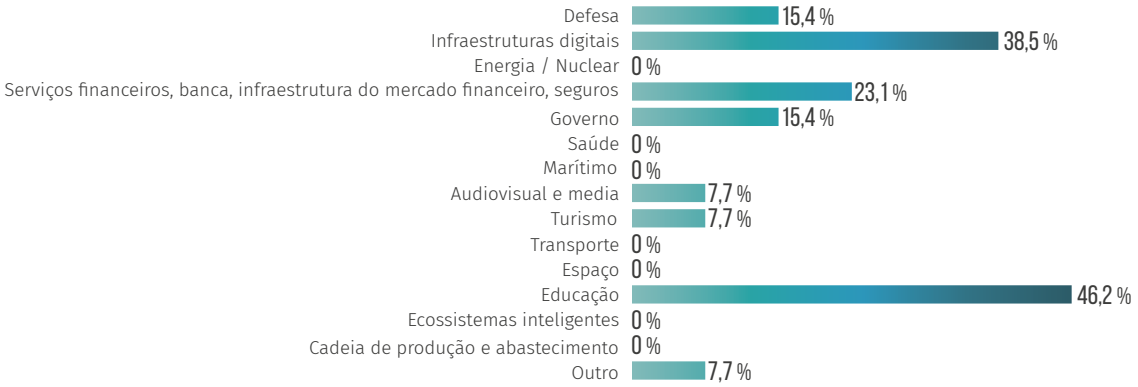


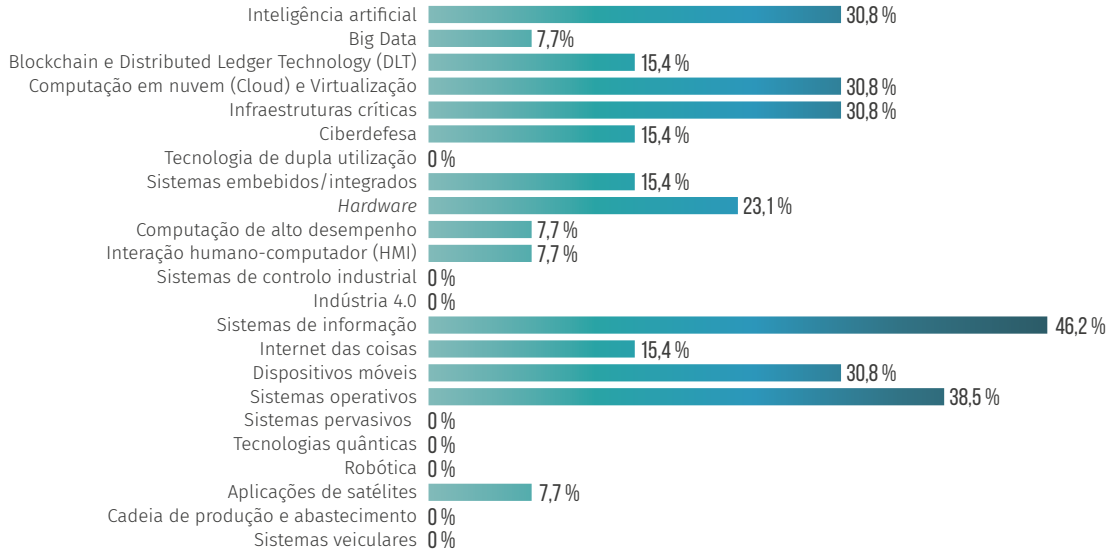
FIGURA 3.49: D12: SETORES DA ECONOMIA, APLICAÇÕES E TECNOLOGIAS.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio dos Fundamentos Teóricos da Análise e de Desenho de Segurança no período entre 2017 e 2021. Uma entidade pode atuar em diferentes setores da economia, áreas de aplicações e tecnologias.

Distribuição dos setores de atividade



Distribuição das aplicações e tecnologias

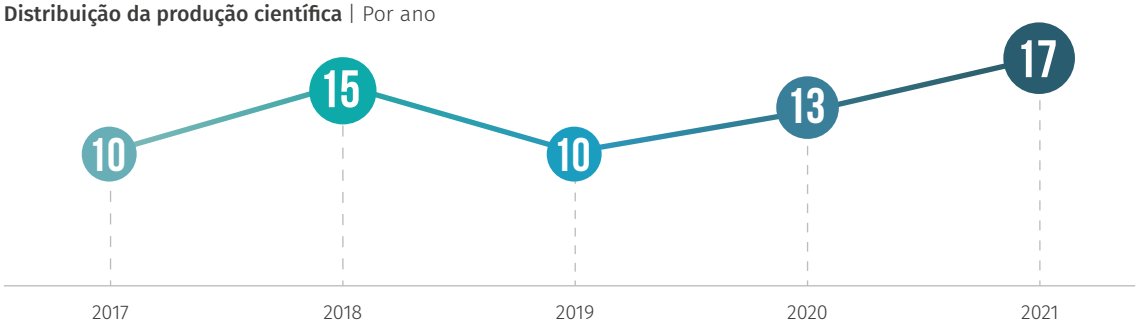


Por se tratar de um domínio de competências significativamente ligado com as ciências fundamentais, é notável o volume de publicações de caráter científico produzido no âmbito de instituições nacionais. Mais especificamente, investigadores afiliados a 19 instituições nacionais estiveram envolvidos na publicação de 65 documentos deste tipo. Entre estas instituições, destacam-se a Universidade de Coimbra, a Universidade do Porto e a Universidade do Minho. Já na distribuição das publicações ao longo dos cinco anos considerados no estudo, observa-se regularidade na produção, com ligeiro destaque para os anos 2018 e 2021 (ver Figura 3.50).

FIGURA 3.50: D12: DISTRIBUIÇÃO DA PRODUÇÃO CIENTÍFICA.

Número de publicações científicas com autores afiliados a instituições nacionais no domínio dos Fundamentos Teóricos da Análise e de Desenho de Segurança.

Distribuição da produção científica | Por ano



Concentração de publicações científicas no domínio dos Fundamentos Teóricos da Análise e de Desenho de Segurança por instituição nacional. Por exemplo, uma instituição nacional foi responsável por 14 publicações no período.

Distribuição da produção científica | Número de publicações por instituição (2017-2021)

3.13. Gestão de Confiança, Garantia de Segurança e Rastreabilidade

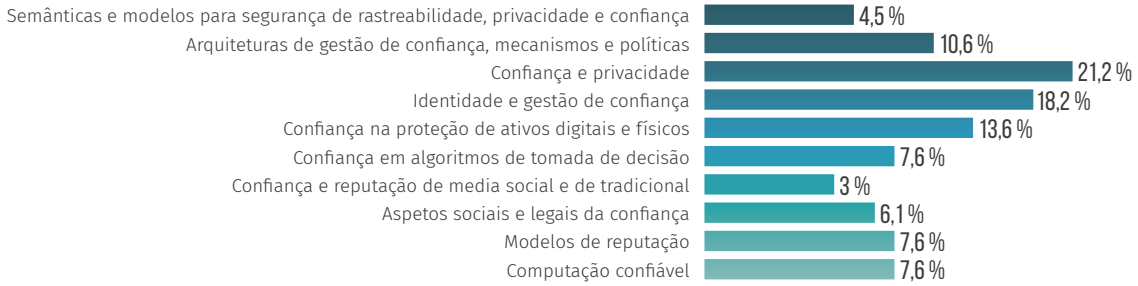
Este domínio de competências em cibersegurança compreende questões de confiança relacionadas com entidades digitais e físicas, tais como, aplicações, serviços, componentes ou sistemas. As abordagens de gestão de confiança podem ser utilizadas para avaliar as garantias de segurança e responsabilização. Do conjunto de entidades participantes do estudo, pouco mais de 7% apontou ter atuação neste domínio, maioritariamente, nas áreas de investigação e do ensino superior. Contudo, destacam-se também as atividades de inovação e de prestação de serviços (ver Figura 3.52). Para todas as áreas, as equipas não passam de três profissionais especializados em 91% das entidades. Já o levantamento exploratório sobre as atividades do tecido empresarial nacional revelou que apenas duas das 120 entidades analisadas apontam algum tipo de serviço ou produto relacionados com este domínio nas suas páginas na Internet.

Quando considerada a distribuição destas atividades entre os subdomínios da taxonomia europeia (ver Figura 3.51), destacam-se:

- Confiança e privacidade;
- Identidade e gestão de confiança;
- Confiança na proteção de ativos digitais e físicos;
- Arquiteturas de gestão de confiança, mecanismos e políticas.

FIGURA 3.51: D13: DISTRIBUIÇÃO POR SUBDOMÍNIO.

Detalhe da atuação das entidades nacionais no domínio da Gestão de Confiança, Garantia de Segurança e Rastreabilidade no período entre 2017 e 2021.



Estas atividades são financiadas, na sua maioria, através de *programas nacionais* ou de *fundos do Estado*. Em concreto, 25% das entidades participantes do estudo indicaram ter participado em projetos nacionais nos últimos cinco anos e outros 25% em projetos de inovação. Além disso, pouco menos de 10% apontou contratos com agências estatais e 16% com o tecido industrial nacional.

De acordo com o repositório do WIPO, três entidades nacionais estiveram envolvidas nos desenvolvimentos que resultaram na obtenção de cinco registos de patentes neste domínio nos últimos cinco anos. Todas as patentes estão relacionadas com métodos de proteção de ativos físicos por meio de métodos e mecanismos digitais. Entre as instituições envolvidas nestes trabalhos, uma é da esfera pública, outra é uma instituição de ensino superior e a terceira, responsável por duas patentes, é do setor privado, não constando, contudo, como associada a nenhuma das entidades listadas na Tabela 2.1.

É importante referir que neste domínio há entidades nacionais a desenvolver atividades de cibersegurança direcionadas para os setores da *defesa*, *energia nuclear*, *serviços financeiros* e *saúde*. Isto vem ratificar o caráter crítico que assumem a gestão de confiança, a garantia de segurança e a rastreabilidade nestes domínios (a completa distribuição é descrita na Figura 3.53). Já as tecnologias e aplicações em destaque incluem os *sistemas de informação* e as *infraestruturas críticas*. As tecnologias de *inteligência artificial*, *DLT*, *computação em nuvem* e *virtualização* também merecem destaque, quando comparados com os setores de atividade e as tecnologias objeto de desenvolvimento.

FIGURA 3.52: D13: TIPOS DE ATIVIDADE E FONTES DE FINANCIAMENTO.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio da Gestão de Confiança, Garantia de Segurança e Rastreabilidade no período entre 2017 e 2021.

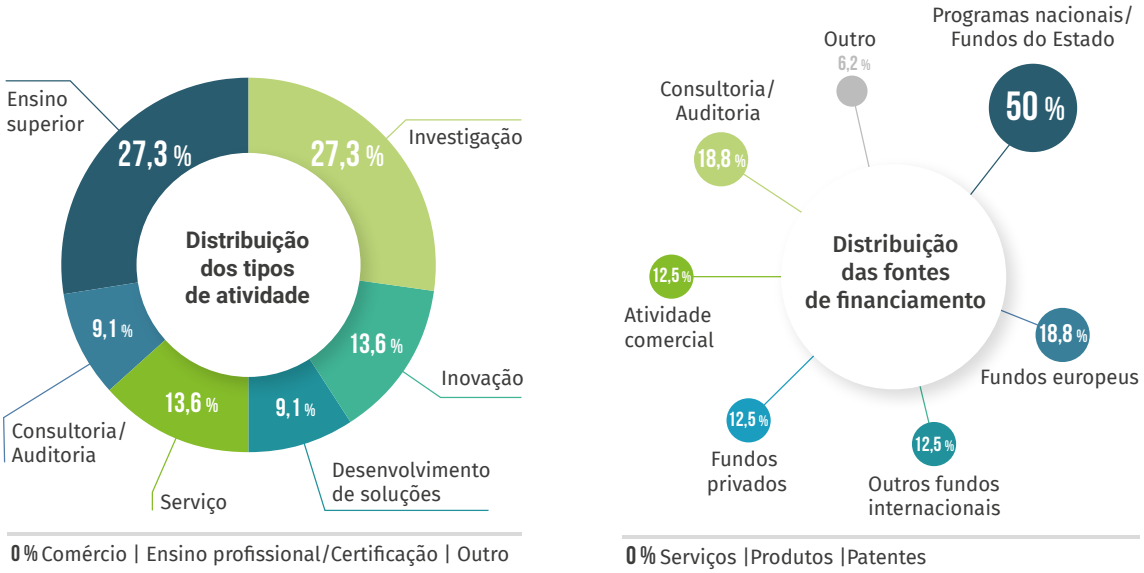
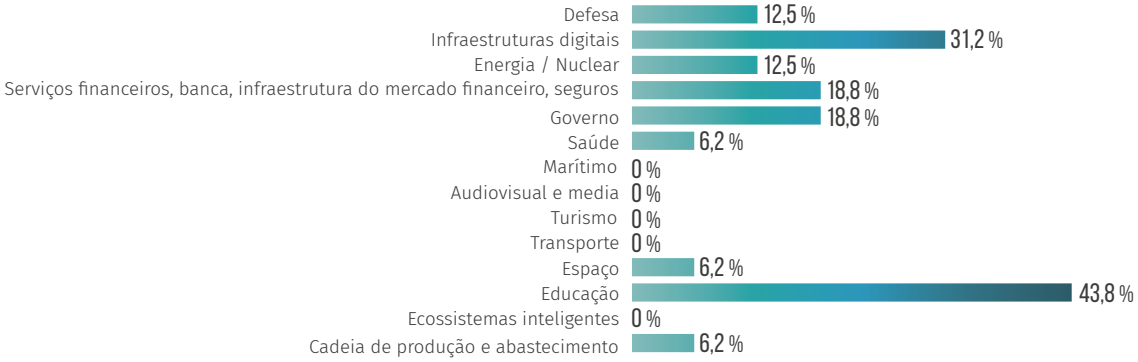


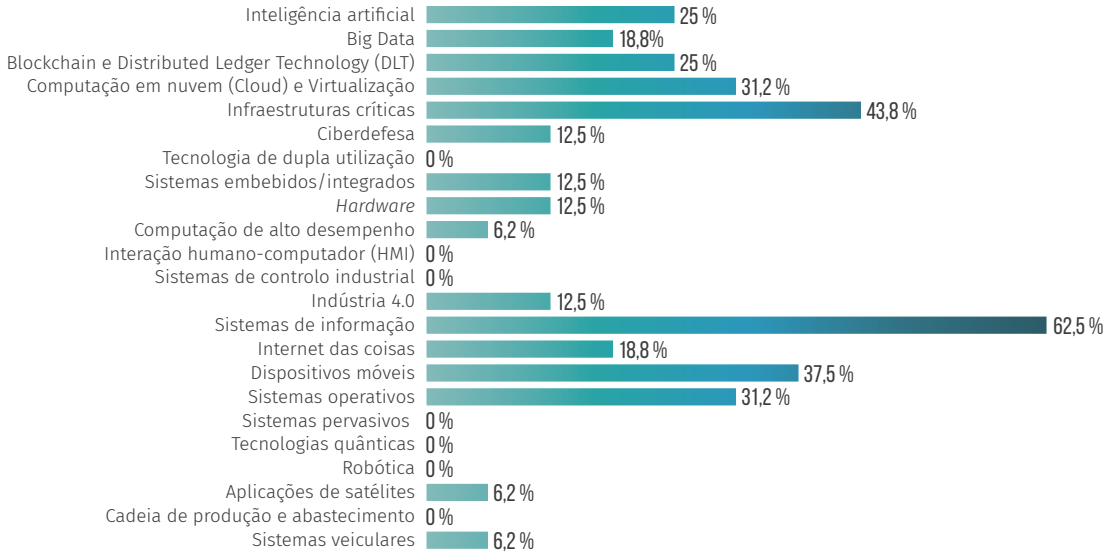
FIGURA 3.53: D13: SETORES DA ECONOMIA, APLICAÇÕES E TECNOLOGIAS.

Respostas dadas pelos representantes das entidades participantes no estudo com atividade no domínio da Gestão de Confiança, Garantia de Segurança e Rastreabilidade no período entre 2017 e 2021. Uma entidade pode atuar em diferentes setores da economia, áreas de aplicações e tecnologias.

Distribuição dos setores de atividade



Distribuição das aplicações e tecnologias

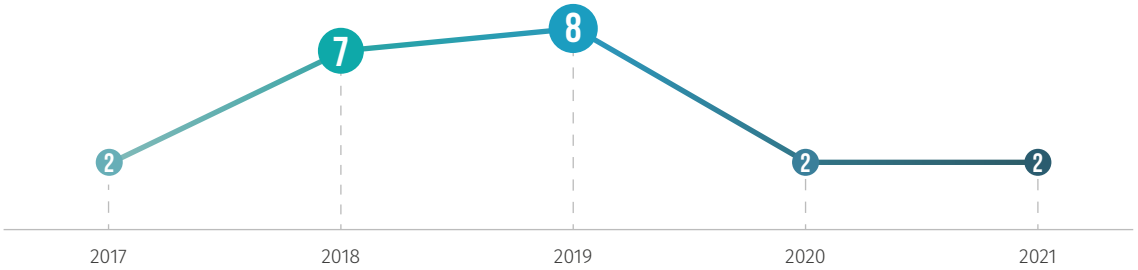


Na vertente da produção de conhecimento e divulgação na forma de artigos de caráter científico, investigadores afiliados a 12 instituições nacionais foram responsáveis por 17 publicações entre o ano 2017 e o ano 2022. Neste período, há um destaque na produção dos anos 2018 e 2019 (ver Figura 3.54), evidenciando-se a Universidade do Porto, a Universidade de Aveiro e a Universidade Nova de Lisboa.

FIGURA 3.54: D13: DISTRIBUIÇÃO DA PRODUÇÃO CIENTÍFICA.

Número de publicações científicas com autores afiliados a instituições nacionais no domínio da Gestão de Confiança, Garantia de Segurança e Rastreabilidade.

Distribuição da produção científica | Por ano



Concentração de publicações científicas no domínio da Gestão de Confiança, Garantia de Segurança e Rastreabilidade por instituição nacional. Por exemplo, uma instituição nacional foi responsável por quatro publicações no período.

Distribuição da produção científica | Número de publicações por instituição (2017-2021)

4. Considerações Finais

Um estudo que tem por objetivo caracterizar a comunidade de competências em cibersegurança depende, em grande parte, da identificação detalhada das entidades com atuação na área, os seus quadros de especialistas, as suas atividades específicas e infraestruturas de suporte. Contudo, dada a sensibilidade do tema, é comum que tais entidades optem por não revelar detalhes que são relevantes para uma caracterização pormenorizada.

Apesar dos desafios suscitados por aquela circunstância, as escolhas metodológicas que sustentam este estudo permitiram descrever o panorama nacional da atividade em cibersegurança nos diferentes setores económicos. Ao combinar o uso de questionários direcionados com o levantamento sistemático de dados de domínio público, foi possível enriquecer a análise e revelar como os interesses e atividades da comunidade nacional de cibersegurança estão distribuídos, quais as fontes principais de financiamento que as fomentam e em que tópicos está concentrada a produção intelectual.

A relevância dos resultados apresentados é ratificada pelo número de entidades participantes no estudo quando comparado com um estudo equivalente de âmbito europeu. Mais especificamente, o Cybersecurity Compentence Survey publicado pela ENISA, que serve como referência continental, contou com a participação de 19 entidades nacionais. Já o presente estudo tem como base de análise as informações fornecidas por 32 entidades com atividades na área de cibersegurança. A diversidade dos setores económicos de atuação das entidades participantes é, também, notavelmente maior no presente estudo.

Considerando a análise global dos resultados, é possível concluir que as entidades que dinamizam a cibersegurança em Portugal são caracterizadas pela predominância de equipas pequenas de especialistas, independentemente do tamanho da entidade (em número de funcionários). Esta realidade espelha o que, na perceção dos autores deste estudo, parece, nuns casos, ser uma deficiente avaliação de risco no domínio da cibersegurança por parte de várias entidades, resultando em recursos humanos subdimensionados e subespecializados nos seus quadros. Noutros casos, parece advir da patente falta de profissionais e dos custos inerentes ao dimensionamento adequado destas equipas. Noutros ainda, parece não estar amadurecida ou não ser economicamente apelativa uma oferta de serviços terceirizados no domínio da cibersegurança. Parece necessário, portanto, o reforço da políticas de capacitação de recursos humanos e aumento da oferta formativa nestes domínios, e a persecução de estratégias de sensibilização do setor privado para a necessidade de assumirem a cibersegurança como parte essencial dos seus processos no contexto da sua organização e do seu negócio. No final do dia, a definição e reforço da implementação de políticas neste domínio deverá resultar de um estímulo ao setor privado de prestação de serviços nestes domínios, como também, por seu turno, num estímulo à transferência de tecnologia e de inovação proveniente das entidades relevantes no contexto científico nacional. Numa futura reedição deste estudo, poderá ser interessante incorporar a dimensão do negócio das empresas (como complemento ao número de colaboradores).

Além disso, há um papel importante dos programas europeus e nacionais de inovação e investigação como fonte de financiamento das atividades relacionadas com a cibersegurança. Aqui, importa realçar a predominância de entidades privadas na captação de recursos via programas europeus, que ultrapassa, em número de entidades, os centros de investigação e as instituições de ensino superior no período entre 2017 e 2021. Já nos programas nacionais, observa-se uma predominância do tecido académico, no mesmo período.

Ainda sobre as fontes de financiamento, é notável a baixa exploração de registos de *software* e de patentes. Esta constatação contrasta com o vigor da produção científica nos cinco anos considerados no estudo. Mesmo em domínios caracterizados por investigação fundamental, e.g., Criptologia e Fundamentos Teóricos da Análise e Desenho de Segurança, observa-se pouca exploração comercial dos resultados obtidos. A este respeito, a perceção dos autores deste estudo é de que, no contexto particular do sistema científico nacional, parece existir por parte de muitos investigadores uma posição de natureza ideológica ou ética académica pouco favorável aos processos de registo de *software* e de patentes. Por outro lado, os custos, a burocracia e a inexperiência nestes processos parecem ser fatores que demovem muitos investigadores e instituições de sequer os tentar iniciar. Se por um lado questões de ideologia ou ética académica,

de convicção individual, dificilmente poderão ser endereçadas pelas políticas públicas, não deixa de ser verdade que se nota um estímulo claro decorrente, por exemplo, dos procedimentos de avaliação de mérito de candidaturas a financiamento de projetos no âmbito nacional e europeu. Nesse sentido, são também evidentes a energia e o investimento já realizado por várias entidades públicas e privadas no sentido de fazerem o melhor uso dos mecanismos existentes de proteção da sua propriedade intelectual. A persecução e o reforço destas políticas parecem ser, portanto, instrumentos importantes no fomento da proteção da propriedade intelectual e na exploração comercial da investigação desenvolvida pelas entidades nacionais nos vários domínios da cibersegurança.

Ao considerar a distribuição das atividades entre os domínios de competências propostos pela taxonomia da ENISA, é possível observar um desalinhamento entre o tecido comercial e o tecido académico. A exceção é o domínio relacionado com a Engenharia de Segurança de *Software* e *Hardware*, que corresponde ao mais ativo em ambos os grupos. No âmbito da comunidade de entidades comerciais, este domínio é seguido pelos domínios de Redes e Sistemas distribuídos e Gestão e Governação de Segurança. Já na comunidade académica, descatam-se os domínios da Gestão de Identidade e Acesso e Criptologia.

Outras duas dimensões do perfil da comunidade de competências nacional em cibersegurança estão relacionadas com os setores de atividades e as áreas de aplicação dos respetivos desenvolvimentos. Na dimensão setorial, o maior número de entidades relacionadas com o tecido académico reflete uma maior concentração no setor da Educação. Este setor é seguido pela área da Saúde, que também concentra o maior número de patentes registadas por inventores afiliados a entidades nacionais, e pela área dedicada às Infraestruturas digitais. Já na dimensão das áreas e tecnologias de aplicação, destacam-se os Sistemas de informação, Sistemas Operativos e Infraestruturas Críticas.

Finalmente, uma vertente relevante desta caracterização é o nível de internacionalização das atividades empreendidas pela comunidade nacional. Tal análise é sustentada unicamente pelo levantamento da produção científica de investigadores ligados a entidades portuguesas. Ao contabilizar o número de coautores e a nacionalidade das respetivas entidades de afiliação, foi possível observar um maior destaque para colaborações com entidades não europeias. Em particular, as entidades sediadas no Brasil e nos Estados Unidos da América corresponderam ao maior volume de colaborações no período considerado. Contudo, observa-se também uma grande heterogeneidade de colaborações envolvendo investigadores afiliados a entidades de mais de 20 países.

É manifesto o processo de progressiva internacionalização da economia, da investigação e da inovação nacional ao longo das últimas décadas. Este é, no entanto, um processo contínuo e particularmente fundamental nos domínios da cibersegurança pelo que, no entendimento dos autores deste estudo, deve ser alvo da atenção particular das políticas públicas dirigidas ao setor da economia e ao sistema científico e tecnológico nacional.

Apesar de esta secção procurar sumariar alguns dos aspetos centrais da caracterização da comunidade portuguesa de competências em cibersegunça, há, certamente, diferentes interpretações alinhadas com os interesses particulares do leitor ou de um setor. Assim, estas considerações finais não pretendem encerrar o estudo. Pelo contrário, têm por objetivo convidar o leitor a uma análise mais orientada aos seus propósitos.

5. ANEXOS

A. INQUÉRITO ON-LINE

a. Grupo 1

1. Nome da instituição

.....

2. País de Origem

- ○ Portugal
- ○ Outro .....

3. Estatuto Jurídico

- ○ Público
- ○ Privado
- ○ Parceria Público-Privada
- ○ Outro .....

4. Tipo de entidade

- ○ Instituição de ensino superior
- ○ Centro de investigação
- ○ Ensino profissional / Certificação
- ○ Comércio de produtos de *software*, appliances, etc.
- ○ Comércio de serviços
- ○ Consultoria
- ○ Administração pública
- ○ Outro .....

5. Número total de colaboradores/ empregados a tempo inteiro

- ○ 1-10
- ○ 11-50
- ○ 51-200
- ○ 201-500
- ○ Mais de 500

6. Número total de colaboradores/ empregados dedicados a cibersegurança

- ○ 0
- ○ 1-3
- ○ 4-10
- ○ 11-20
- ○ 21-50
- ○ Mais de 50

7. Fontes de financiamento das atividades em cibersegurança

- ○ Programas nacionais / Fundos do Estado
- ○ Fundos europeus
- ○ Outros fundos internacionais
- ○ Fundos privados
- ○ Atividade comercial
- ○ Serviços
- ○ Consultoria / Auditoria
- ○ Produtos
- ○ Patentes
- ○ Outro .....

8. Atividade em cibersegurança

- ○ Ensino superior
- ○ Ensino profissional / Certificação
- ○ Investigação
- ○ Desenvolvimento de soluções (*software*, políticas, etc.)
- ○ Consultoria
- ○ Comércio
- ○ Gestão de Infraestruturas
- ○ Outro .....

9. Os domínios de cibersegurança neste inquérito estão alinhados com a taxonomia da European Union Agency for Cybersecurity (ENISA) para os domínios de competências em cibersegurança.

9.a. Garantia, Auditoria e Certificação

- O Garantia
- O Auditoria
- O Avaliação
- O Certificação
- O Perfil de proteção
- O Alvo de segurança
- O Outro .....

9.b. Criptologia

- O Assinaturas digitais
- O Criptografia assimétrica e criptoanálise
- O Criptografia simétrica e criptoanálise
- O Funções de hash
- O Gestão de chaves
- O Autenticação de mensagens
- O Geração de números aleatórios
- O Metodologias, técnicas e ferramentas de criptoanálise
- O Criptologia quântica
- O Criptologia pós-quântica
- O Fundamentos matemáticos da criptografia
- O Outro .....

9.c. Segurança de Dados e Privacidade

- O Requisitos de privacidade para sistemas de gestão de dados
- O Conceção, implementação e operação de sistemas de gestão de dados que incluam segurança e privacidade
- O Pseudo-anonimato
- O Desvinculação
- O Privacidade por definição e tecnologias para melhoria da privacidade
- O Gestão de Direitos Digitais (DRM)
- O Controlo do uso de dados
- O Outro .....

9.d. Tratamento/Resposta de Incidentes Operacionais e Forense Digital

- O Teorias, técnicas e ferramentas para a identificação, recolha, aquisição e preservação de provas digitais
- O Processos forenses digitais e modelos de fluxo de trabalho
- O Estudos de casos forenses digitais
- O Questões legais, éticas e políticas relacionadas com forense digital
- O Previsão de incidentes baseada em inteligência
- O Outro .....

9.e. Fatores Humanos

- O Acessibilidade
- O Usabilidade
- O Engenharia social e outros riscos relacionados com utilizadores
- O Segurança sócio-técnica
- O Erros humanos
- O Melhoria da perceção de risco
- O Modelos psicológicos
- O Aceitação pelos utilizadores de políticas e tecnologias de segurança
- O Automatização das funcionalidades de segurança
- O Segurança não-intrusiva
- O Preocupações e comportamentos individuais, organizacionais e de grupo em matéria de privacidade da informação
- O Motivadores e inibidores do uso indevido de informação privilegiada
- O Impactos das normas, políticas, requisitos de conformidade
- O Governança organizacional para garantia da informação
- O Atitudes e práticas de privacidade
- O Ética e segurança informática
- O Segurança transparente
- O Caracterização de atacantes
- O Outro .....

9.f. Gestão de Identidade e Acesso

- O Modelos de gestão da identidade, estruturas, aplicações, tecnologias e ferramentas (e.g., PKI, RFID, SSO, etc)
- O Protocolos e estruturas para o controlo de acesso (autenticação e autorização)
- O Garantia de qualidade da gestão da identidade
- O eIDAS
- O Segurança de documentos ópticos e electrónicos
- O Aspetos legais da gestão de identidade
- O Aplicação da lei e gestão de identidade
- O Métodos, tecnologias e ferramentas biométricas
- O Outro

9.g. Gestão e Governação de Segurança

- O Gestão de Risco
- O Monitorização contínua
- O Modelação de ameaças e de vulnerabilidades
- O Modelação de ataques e de contramedidas
- O Aspetos de gestão relativos a segurança de informação
- O Avaliação de eficácia de informação de segurança de informação e graus de controlo
- O Identificação do impacto de alterações de *hardware* e de *software* na gestão da Segurança de Informação
- O Normas para Segurança de Informação
- O Gestão de incidentes e recuperação de desastres
- O Reporte (e.g. recuperação de desastres e continuidade de negócio)
- O Análise teórica e empírica do comportamento da segurança de informação
- O Adoção, uso e continuidade de tecnologias e políticas de segurança de informação
- O Conformidade com políticas, procedimentos e regulamentos de segurança de informação
- O Procedimentos de verificação de membros e colaboradores de equipas de segurança
- O Aspetos económicos do ecossistema de cibersegurança
- O Outro .....

9.h. Rede e Sistemas Distribuídos

- O Princípios, métodos e tecnologias de segurança para redes
- O Princípios, métodos e tecnologias de segurança em sistemas distribuídos
- O Aspetos gerenciais, procedimentais e técnicos de segurança de rede
- O Requisitos para segurança de rede
- O Segurança de redes de telecomunicações
- O Protocolos e frameworks para computação segura distribuída
- O Ataques a camadas de rede e técnicas de mitigação
- O Análise de propagação de ataques de rede
- O Análise e simulação de segurança de sistemas distribuídos
- O Técnicas de consenso distribuído
- O Modelos de tolerância a faltas
- O Computações seguras distribuídas
- O Outro .....

9.i. Engenharia de Segurança de *software* e de *hardware*

- O Engenharia de requisitos de segurança com ênfase em identidade, privacidade, rastreabilidade e confiança
- O Análise de segurança e de risco de composições de componentes
- O Arquiteturas e desenho de *software* seguro
- O Padrões de desenho de segurança
- O Princípios e melhores práticas práticas de programação segura
- O Suporte de segurança em ambientes de programação
- O Documentação de segurança
- O Refinamento e verificação de modelos de política de gestão de segurança
- O Verificação e imposição de segurança em tempo de execução
- O Monitorização contínua
- O Testagem e validação de segurança
- O Descoberta de vulnerabilidades e testes de penetração
- O Garantia quantitativa de segurança
- O Deteção de intrusão e honeypots
- O Análise de *software* malicioso
- O Segurança orientada por modelos e linguagens de modelação de domínio específico
- O Sistemas auto-regeneráveis
- O Outro .....

9.j. Medidas de Segurança

- O Segurança analítica
- O Métricas de segurança
- O Frameworks de validação e comparação para métricas de segurança
- O Medição e avaliação de níveis de segurança
- O Outro .....

9.k. Tecnologia e Aspectos Legais

- O Acusação de cibercrime e aplicação da lei
- O Cibersegurança e ética
- O Direitos de propriedade intelectual
- O Análise e desenho de regulamentação de cibersegurança
- O Investigação de crimes informáticos (cibercrime) e violações de segurança
- O Aspetos legais, societais e éticos em segurança de informação
- O Aspetos legais de certificação
- O Media social
- O Outro .....

9.l. Fundamentos Teóricos da Análise e de Desenho de Segurança

- O Especificação e verificação formal de vários aspetos da segurança (confidencialidade, integridade, autenticação e disponibilidade)
- O Técnicas formais para a análise, verificação e auditoria de *software* e *hardware*
- O Modelação de fluxo de informação e sua aplicação em políticas de confidencialidade, na composição de sistemas e análise de canais dissimulados
- O Novas técnicas baseadas em teoria para a análise e desenho de protocolos criptográficos e suas aplicações
- O Verificação formal e garantia de segurança
- O Outro .....

9.m. Gestão de Confiança, Garantia de Segurança e Rastrear

- O Semânticas e modelos para segurança de rastreabilidade, privacidade e confiança
- O Arquiteturas de gestão de confiança, mecanismos e políticas
- O Confiança e privacidade
- O Identidade e gestão de confiança
- O Confiança na proteção de ativos digitais e físicos
- O Confiança em algoritmos de tomada de decisão
- O Confiança e reputação de media social e de tradicional
- O Aspetos sociais e legais da confiança
- O Modelos de reputação
- O Computação confiável
- O Outro .....

b. Grupos 2-14

Para cada domínio selecionado entre as questões *9a* e *9m*, o inquirido tem de responder ao seguinte grupo de questões relativo a cada domínio.

1. Número total de profissionais envolvidos nesta área

- ○ 1-3
- ○ 4-10
- ○ 11-20
- ○ 21-50
- ○ Mais de 50

2. Número total de profissionais envolvidos nesta área

- ○ Investigação
- ○ Inovação
- ○ Desenvolvimento de soluções
- ○ Serviço
- ○ Consultoria / Auditoria
- ○ Comércio
- ○ Ensino superior
- ○ Ensino profissional / Certificação
- ○ Outro .....

3. Número total de profissionais envolvidos nesta área

- ○ Inteligência artificial
- ○ Big Data
- ○ Blockchain e Distributed Ledger Technology (DLT)
- ○ Computação em nuvem (Cloud) e Virtualização
- ○ Infraestruturas críticas
- ○ Ciberdefesa
- ○ Tecnologia de dupla utilização
- ○ Sistemas embebidos/integrados
- ○ *Hardware*
- ○ Computação de alto desempenho
- ○ Interação humano-computador (HMI)
- ○ Sistemas de controlo industrial
- ○ Indústria 4.0
- ○ Sistemas de informação
- ○ Internet das coisas
- ○ Dispositivos móveis
- ○ Sistemas operativos
- ○ Sistemas pervasivos
- ○ Tecnologias quânticas
- ○ Robótica
- ○ Aplicações de satélites
- ○ Cadeia de produção e abastecimento
- ○ Sistemas veiculares
- ○ Outro .....

4. Setores onde a atividade de cibersegurança é aplicada

- ○ Defesa
- ○ Infraestrutura digital
- ○ Energia / Nuclear
- ○ Serviços financeiros, banca, infraestrutura do mercado financeiro, seguros
- ○ Governo
- ○ Saúde
- ○ Marítimo
- ○ Audiovisual e media
- ○ Turismo
- ○ Transporte
- ○ Espaço
- ○ Educação
- ○ Ecossistemas inteligentes
- ○ Cadeia de produção e abastecimento
- ○ Outro

5. Principais fontes de financiamento desta atividade

- ○ Programas nacionais / Fundos do Estado
- ○ Fundos europeus
- ○ Outros fundos internacionais
- ○ Fundos privados
- ○ Atividade comercial
- ○ Serviços
- ○ Consultoria / Auditoria
- ○ Produtos
- ○ Patentes
- ○ Outro .....

6. Número de projetos europeus

- ○ 0
- ○ 1-3
- ○ 4-10
- ○ 11-20
- ○ Mais de 20

7. Número de projetos nacionais de investigação

- ○ 0
- ○ 1-3
- ○ 4-10
- ○ 11-20
- ○ Mais de 20

8. Número de projetos de inovação

- ○ 0
- ○ 1-3
- ○ 4-10
- ○ 11-20
- ○ Mais de 20

9. Número de patentes concedidas

- ○ 0
- ○ 1-3
- ○ 4-10
- ○ 11-20
- ○ Mais de 20

10. Número de acordos / contratos com a indústria

- ○ 0
- ○ 1-3
- ○ 4-10
- ○ 11-20
- ○ Mais de 20

11. Número de acordos / contratos com a governo

- ○ 0
- ○ 1-3
- ○ 4-10
- ○ 11-20
- ○ Mais de 20

12. Número de memorandos de entendimento com outras organizações

- ○ 0
- ○ 1-3
- ○ 4-10
- ○ 11-20
- ○ Mais de 20

13. Número de artigos científicos publicados em revistas ou eventos com mediação por pares

- ○ 0
- ○ 1-3
- ○ 4-10
- ○ 11-20
- ○ Mais de 20

14. Número de registos de *software*

- ○ 0
- ○ 1-3
- ○ 4-10
- ○ 11-20
- ○ Mais de 20

B. DOMÍNIOS E SUBDOMÍNIOS DA TAXONOMIA DA ENISA

D01 - GARANTIA, AUDITORIA E CERTIFICAÇÃO

Subdomínios:

- Garantia
- Auditoria
- Avaliação
- Certificação
- Perfil de proteção
- Alvo de segurança

D02 - CRIPTOLOGIA

Subdomínios:

- Assinaturas digitais
- Criptografia assimétrica e criptoanálise
- Criptografia simétrica e criptoanálise
- Funções de hash
- Gestão de chaves
- Autenticação de mensagens
- Geração de números aleatórios
- Metodologias, técnicas e ferramentas de criptoanálise
- Criptologia quântica
- Criptologia pós-quântica
- Fundamentos matemáticos da criptografia

D03 - SEGURANÇA DE DADOS E PRIVACIDADE

Subdomínios:

- Requisitos de privacidade para sistemas de gestão de dados
- Conceção, implementação e operação de sistemas de gestão de dados que incluam segurança e privacidade
- Pseudo-anonimato
- Desvinculação
- Privacidade por definição e tecnologias para melhoria da privacidade
- Gestão de Direitos Digitais (DRM)
- Controlo do uso de dados

D04 - TRATAMENTO/RESPOSTA DE INCIDENTES OPERACIONAIS E FORENSE DIGITAL

Subdomínios:

- Teorias, técnicas e ferramentas para a identificação, recolha, aquisição e preservação de provas digitais
- Processos forenses digitais e modelos de fluxo de trabalho
- Estudos de casos forenses digitais
- Questões legais, éticas e políticas relacionadas com forense digital
- Previsão de incidentes baseada em inteligência

D05 - FATORES HUMANOS

Subdomínios:

- Acessibilidade
- Usabilidade
- Engenharia social e outros riscos relacionados com utilizadores
- Segurança sócio-técnica
- Erros humanos
- Melhoria da perceção de risco
- Modelos psicológicos
- Aceitação pelos utilizadores de políticas e tecnologias de segurança
- Automatização das funcionalidades de segurança
- Segurança não-intrusiva
- Preocupações e comportamentos individuais, organizacionais e de grupo em matéria de privacidade da informação
- Motivadores e inibidores do uso indevido de informação privilegiada
- Impactos das normas, políticas, requisitos de conformidade
- Governança organizacional para garantia da informação
- Atitudes e práticas de privacidade
- Ética e segurança informática
- Segurança transparente
- Caracterização de atacantes

D06 - GESTÃO DE IDENTIDADE E ACESSO

Subdomínios:

- Modelos de gestão da identidade, estruturas, aplicações, tecnologias e ferramentas
- Protocolos e estruturas para o controlo de acesso
- Garantia de qualidade da gestão da identidade
- eIDAS
- Segurança de documentos ópticos e electrónicos
- Aspetos legais da gestão de identidade
- Aplicação da lei e gestão de identidade
- Métodos, tecnologias e ferramentas biométricas

D07 - GESTÃO E GOVERNAÇÃO DE SEGURANÇA

Subdomínios:

- Gestão de Risco
- Monitorização contínua
- Modelação de ameaças e de vulnerabilidades
- Modelação de ataques e de contramedidas
- Aspetos de gestão relativos a segurança de informação
- Avaliação de eficácia de informação de segurança de informação e graus de controlo
- Identificação do impacto de alterações de *hardware* e de *software* na gestão da Segurança de Informação
- Normas para Segurança de Informação
- Gestão de incidentes e recuperação de desastres
- Reporte
- Análise teórica e empírica do comportamento da segurança de informação
- Adoção, uso e continuidade de tecnologias e políticas de segurança de informação
- Conformidade com políticas, procedimentos e regulamentos de segurança de informação
- Procedimentos de verificação de membros e colaboradores de equipas de segurança
- Aspetos económicos do ecossistema de cibersegurança

D08 - REDE E SISTEMAS DISTRIBUÍDOS

Subdomínios:

- Princípios, métodos e tecnologias de segurança para redes
- Princípios, métodos e tecnologias de segurança em sistemas distribuídos
- Aspetos gerenciais, procedimentais e técnicos de segurança de rede
- Requisitos para segurança de rede
- Segurança de redes de telecomunicações
- Protocolos e frameworks para computação segura distribuída
- Ataques a camadas de rede e técnicas de mitigação
- Análise de propagação de ataques de rede
- Análise e simulação de segurança de sistemas distribuídos
- Técnicas de consenso distribuído
- Modelos de tolerância a faltas
- Computações seguras distribuídas

D09 - ENGENHARIA DE SEGURANÇA DE *SOFTWARE* E DE *HARDWARE*

Subdomínios:

- Engenharia de requisitos de segurança com ênfase em identidade, privacidade, rastreabilidade e confiança
- Análise de segurança e de risco de composições de componentes
- Arquiteturas e desenho de *software* seguro
- Padrões de desenho de segurança
- Princípios e melhores práticas de programação segura
- Suporte de segurança em ambientes de programação
- Documentação de segurança
- Refinamento e verificação de modelos de política de gestão de segurança
- Verificação e imposição de segurança em tempo de execução
- Monitorização contínua
- Testagem e validação de segurança
- Descoberta de vulnerabilidades e testes de penetração
- Garantia quantitativa de segurança
- Deteção de intrusão e honeypots
- Análise de *software* malicioso
- Segurança orientada por modelos e linguagens de modelação de domínio específico
- Sistemas auto-regeneráveis

D10 - MEDIDAS DE SEGURANÇA

Subdomínios:

- Segurança analítica
- Métricas de segurança
- Frameworks de validação e comparação para métricas de segurança
- Medição e avaliação de níveis de segurança

D11 - TECNOLOGIA E ASPETOS LEGAIS

Subdomínios:

- Acusação de cibercrime e aplicação da lei
- Cibersegurança e ética
- Direitos de propriedade intelectual
- Análise e desenho de regulamentação de cibersegurança
- Investigação de crimes informáticos (cibercrime) e violações de segurança
- Aspetos legais, societais e éticos em segurança de informação
- Aspetos legais de certificação
- Media social

D12 - FUNDAÇÕES TEÓRICAS DA ANÁLISE E DE DESENHO DE SEGURANÇA

Subdomínios:

- Especificação e verificação formal de vários aspetos da segurança (confidencialidade, integridade, autenticação e disponibilidade)
- Técnicas formais para a análise, verificação e auditoria de *software* e *hardware*
- Modelação de fluxo de informação e sua aplicação em políticas de confidencialidade, na composição de sistemas e análise de canais dissimulado
- Novas técnicas baseadas em teoria para a análise e desenho de protocolos criptográficos e suas aplicações
- Verificação formal e garantia de segurança

D13 - GESTÃO DE CONFIANÇA, GARANTIA DE SEGURANÇA E RASTREABILIDADE

Subdomínios:

- Semânticas e modelos para segurança de rastreabilidade, privacidade e confiança
- Arquiteturas de gestão de confiança, mecanismos e políticas
- Confiança e privacidade
- Identidade e gestão de confiança
- Confiança na proteção de ativos digitais e físicos
- Confiança em algoritmos de tomada de decisão
- Confiança e reputação de media social e de tradicional
- Aspetos sociais e legais da confiança
- Modelos de reputação
- Computação confiável

C. DIMENSÃO SETORIAL DO ESTUDO

No âmbito da proposta de taxonomia das competências em cibersegurança proposta pela ENISA, há uma dimensão de classificação que corresponde aos setores de atividades onde a cibersegurança é aplicada. O presente estudo adota esta classificação e, por esta razão, transcreve a definição de cada setor. Pretende-se, com isso, uma melhor caracterização da distribuição das atividades e dos grupos de competências no contexto nacional.

DEFESA

Este setor abrange as atividades e infraestruturas necessárias à proteção dos cidadãos, incluindo a utilização de sistemas aeronáuticos, espaciais, eletrónicos, terrestres ou de telecomunicações.

INFRAESTRUTURAS DIGITAIS

Este setor inclui empresas que fornecem serviços e plataformas digitais, incluindo serviços em nuvem para armazenamento de dados e fornecedores de serviços web. Engloba também o conjunto de empresas e serviços de fornecimento de Internet, bem como as infraestruturas necessárias para realizar tais comunicações (e.g., fornecedores de serviços DNS).

ENERGIA / NUCLEAR

Este setor inclui as empresas e organizações destinadas à produção e distribuição de energia, incluindo eletricidade, petróleo ou gás. Inclui a infraestrutura necessária para estas atividades, tais como operadores de sistemas de distribuição/armazenamento/transmissão, operadores de produção de energia, ou contadores e equipamentos inteligentes.

No âmbito da produção nuclear, este setor engloba o conjunto de atividades relacionadas com a segurança nuclear, resíduos radioativos e combustível irradiado, proteção contra radiações, desativação de instalações nucleares, bem como a implementação de salvaguardas para evitar a utilização indevida.

SERVIÇOS FINANCEIROS

Este setor abrange as instituições destinadas a fornecer serviços financeiros, tais como, serviços bancários, de seguros ou de corretagem, além de infraestruturas destinadas ao mercado financeiro.

GOVERNO

Este setor refere-se ao conjunto de sistemas e atividades para implementar serviços governamentais mais eficientes (e.g., eVoting, estratégia de cibersegurança, políticas públicas, previsões e identificação de tendências), com o objetivo de aumentar a transparência e a participação dos cidadãos na vida política. Inclui também outros serviços governamentais (e.g., segurança de fronteiras, combate ao crime e ao terrorismo).

SAÚDE

Este setor inclui as empresas relacionadas com o fabrico de dispositivos médicos (e.g., dispositivos médicos implantáveis), a indústria farmacêutica, bem como os estabelecimentos de saúde, incluindo hospitais e clínicas privadas. Compreende também as atividades relativas à monitorização de doenças crónicas e pessoas idosas, com base na integração de novas tecnologias no ecossistema dos cuidados de saúde (e.g., saúde inteligente).

AUDIOVISUAL E MEDIA

Este setor abrange serviços de comunicação social tradicionais, tais como a rádio, televisão e cinema, mas também novos meios de comunicação social, que vão desde publicações digitais a serviços em linha, incluindo redes sociais.

TRANSPORTE

Este setor envolve o conjunto de atividades relacionadas com o movimento de seres humanos, animais ou objetos entre dois pontos. Este movimento pode ser realizado por diferentes meios (e.g., ar, terra ou água) e pode envolver diferentes componentes de infraestrutura (e.g., operadores de gestão de tráfego ou autoridades rodoviárias), veículos (e.g., automóveis, aviões ou navios) e operações, tais como a gestão e supervisão das entidades de infraestrutura.

ESPAÇO

Este setor refere-se ao conjunto de atividades para fomentar a criação de programas específicos para a exploração do espaço. Tais programas e indústrias espaciais são responsáveis por implementar a funcionalidade necessária à realização de tais atividades, incluindo serviços de navegação e tempo, observação da Terra, ou a utilização de fornecedores de dados de satélite.

CADEIA DE PRODUÇÃO E ABASTECIMENTO

Este setor inclui uma vasta gama de atividades de cadeia de fornecimento e técnicas de produção, desde pequenas empresas que utilizam técnicas de produção tradicionais, a empresas de muito grande dimensão que se encontram no topo de uma pirâmide alta e ampla de fornecedores de peças e componentes, que fabricam coletivamente produtos complexos (e.g., integração de sistemas ou produtos).