CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

RELATÓRIO

CIBERSEGURANÇA EM PORTUGAL

ECONOMIA | MAIO 2022

Observatório
de **Cibersegurança**

RELATÓRIO CIBERSEGURANÇA EM PORTUGAL

ECONOMIA

MAIO 2022

AUTORES

FRANCISCO CARBALLO-CRUZ (Coordenação)
NIPE | UNIVERSIDADE DO MINHO

JOÃO CEREJEIRA
NIPE | UNIVERSIDADE DO MINHO

ROSA-BRANCA ESTEVES
NIPE | UNIVERSIDADE DO MINHO

APOIO

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

IAPMEI
Parcerias para o Crescimento

COLABORAÇÃO

BÁRBARA ROCHA
UNIVERSIDADE DO MINHO

NIPE
Núcleo de Investigação em Políticas Económicas e Empresariais

DESIGN EDITORIAL

TWF
DESIGN STUDIO

TWOFOLD DESIGN STUDIO
HTTPS://TWOFOLD.PT
BRAGA | PORTUGAL
GERAL@TWOFOLD.PT

ÍNDICE

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

Índice de Figuras (Continuação)

Índice de Figuras (Continuação)

TERMOS, SIGLAS E ABREVIATURAS

AP2SI – Associação Portuguesa para a Promoção da Segurança de Informação	INE – Instituto Nacional de Estatística
B2B – *Business-to-Business*	EC3 – Centro Europeu de Cibercriminalidade
B2C – *Business-to-Consumer*	ECSO – Organização Europeia de Cibersegurança
B2G – *Business-to-Government*	eIDAS – Sistema de Identificação e Autenticação Eletrónica à Escala Europeia
CAE – Classificação das Atividades Económicas	EMGFA – Estado Maior General das Forças Armadas
CERT.EU – Equipa de Resposta a Emergências Informáticas para as Instituições Europeias	EMPACT – Plataforma Multidisciplinar Europeia Contra as Ameaças Criminosas
CERT.PT – Equipa de Reposta a Incidentes de Segurança Informática Nacional	ENISA – Agência Europeia para a Segurança das Redes e da Informação
CISO – *Chief Information Security Officer*	ERP – *Enterprise Resource Planning* – *Planeamento de Recursos Empresariais*
CMR – *Customer Relationship Management* – Gestão de Relacionamento com Clientes	EUA – Estados Unidos da América
CNCS – Centro Nacional de Cibersegurança	FED – Fundo Europeu de Defesa
CSIRT – Equipas Nacionais de Resposta a Emergências	GCA – Agenda Global de Cibersegurança
CSO – *Chief Executive Officers*	GCI – Índice Global de Cibersegurança
DDoS – *Distributed Denial of Services*	GNS – Gabinete Nacional de Cibersegurança
DGAE – Direção Geral da Administração Escolar	IA, AI – Inteligência Artificial
DOS – *Disk Operating System*	IAPMEI – Agência para a Competitividade e Inovação
IoT – *Internet of Things* – Internet das Coisas	QNR-CS – Quadro Nacional de Referência de Cibersegurança
ISAC – *Information Sharing and Analysis Centers* – Centros de Análise e Partilha de Informação	RNCSIRT – Rede Nacional de CSIRT
ISO – *International Organization for Standardization*	SCADA – Sistemas de Supervisão e Aquisição de Dados
ITSEC – Administração de Segurança em Sistemas de Informação	SIRP – Sistema de Informações da República Portuguesa
ITSO – *International Telecommunications Satellite Organization*	SPAM – *Sending and Posting Advertisement in Mass*
ISP – Fornecedores de Serviços de Internet	SRI – Segurança de Redes e Sistemas de Informação
ITU – União Internacional de Telecomunicações	TeSP – Curso Técnico Superior Profissional
LVT – Lisboa e Vale do Tejo	TI, IT – Tecnologia da Informação
ML – Machine Learning	TIC – Tecnologias da Informação e Comunicação
NATO – Organização do Tratado do Atlântico Norte	UE, EU – União Europeia
NUT – Nomenclatura das Unidades Territoriais para Fins Estatísticos	UE-27 – Estados Membros da União Europeia
OCDE – Organização para a Cooperação e Desenvolvimento Económico	UN – Organização das Nações Unidas
PIB – Produto Interno Bruto	UNC3T – Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária
PIC – Proteção de Infraestruturas Críticas	v.a. – Valor Acrescentado
PME – Pequenas e Médias Empresas	VPN – *Virtual Private Network*
PPP – Parceria Público-Privada	WEF – *World Economic Forum*

AGRADECIMENTOS

A realização deste estudo contou com o apoio de diversas entidades e pessoas. O nosso maior agradecimento é para o Observatório de Cibersegurança, nomeadamente para os profissionais que, ao longo dos meses de realização do estudo, nos foram dando orientações preciosas, fornecendo dados e documentos de interesse, disponibilizando contactos valiosos e, sobretudo, disciplinando o andamento dos trabalhos e das entregas parcelares com que nos tínhamos comprometido.

Devemos um agradecimento institucional ao IAPMEI, por nos ter apoiado na realização do inquérito às PMEs. Deixamos também uma palavra de gratidão ao Dr. José Augusto Vale e às Dras. Helena Laymé e Júlia Tomaz, que comentaram o inquérito inicial, sugeriram abordagens de aplicação e garantiram uma taxa de resposta muito acima da inicialmente prevista. Agradecemos também à Dra. Maria Jordão, da DGAE, por elucidar-nos sobre a disponibilidade de dados estatísticos em algumas áreas, ao Eng. Jorge Pinto, da Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI), por fornecer-nos dados sobre os profissionais de cibersegurança, e ao Dr. Miguel Guimarães, da Associação Portuguesa de Seguradores, por partilhar o seu conhecimento sobre a interação entre cibersegurança e seguros.

Por último, justifica-se uma palavra aos membros do Conselho Consultivo do Observatório de Cibersegurança, Professores Doutores Manuel Mira Godinho e Sandro Miguel Mendonça, que tiveram a gentileza de discutir connosco, numa fase ainda preliminar dos trabalhos, o seu entendimento do pretendido e as diferentes formas de abordar as temáticas que vinculam a economia e a cibersegurança.

A todos, o nosso bem-haja!


01
01
01
01

SUMÁRIO EXECUTIVO

Este relatório aborda a dimensão económica da cibersegurança, no entanto, está especialmente centrado na problemática da cibersegurança nas empresas. Do lado da oferta, o estudo dimensiona e caracteriza o setor da cibersegurança em Portugal, e do lado da procura, caracteriza e analisa os níveis de exposição e as políticas, práticas e protocolos de cibersegurança nas empresas portuguesas, especialmente nas de pequena e média dimensão. Simultaneamente, enquadra os riscos cibernéticos e a sua gestão, analisa o quadro institucional e o ambiente regulatório e caracteriza a situação das empresas portuguesas em matéria de exposição digital e cibersegurança no contexto da União Europeia. No âmbito do estudo recorreu-se a uma exaustiva *desk research* e a análise de dados secundários de diversas fontes. Os dados primários utilizados no relatório procedem de inquéritos promovidos ou com o apoio do Observatório de Cibersegurança do Centro Nacional de Cibersegurança.

PANORAMA GLOBAL

PANORAMA GLOBAL

A. FACTOS E TENDÊNCIAS

I. FUNDAMENTOS ECONÓMICOS

Uma parte significativa dos problemas de cibersegurança tem caráter económico. O grande crescimento dos incidentes de cibersegurança é, em grande medida, explicado por um conjunto de barreiras de natureza económica, que impedem que o investimento em cibersegurança alcance níveis eficientes. A falta de alinhamento dos incentivos, as assimetrias de informação e a existência de externalidades[1] são as três principais barreiras que limitam o investimento em segurança cibernética.

Para limitar os impactos dessas barreiras ao investimento podem ser adotadas diferentes medidas regulatórias: i) A regulação da segurança *ex ante* e a responsabilização ex *post*; ii) A divulgação de informação para reduzir assimetrias; iii) A generalização da adoção de seguros contra riscos cibernéticos; iv) A responsabilização indireta do intermediário; e, inclusivamente v) A promoção de medidas de reconhecimento de boas práticas e protocolos de cibersegurança, nomeadamente, de certificação.

II. RISCOS E AMEAÇAS PARA A ECONOMIA E AS EMPRESAS

O crescimento dos riscos derivados das ameaças à segurança da informação está vinculado ao maior impacto dos ataques e à sua maior probabilidade de ocorrência, que deriva de uma maior exposição da sociedade aos dispositivos digitais. Os riscos associados às falhas de cibersegurança continuam a ser das principais categorias de risco económico e empresarial, a curto e médio prazo, quer à escala global, quer à escala nacional.[2] Na Europa, as principais ameaças cibernéticas são: o *ransomware*, o *malware*, o *cryptojacking*, as ameaças ligadas ao correio eletrónico, as ameaças vinculadas a dados, as ameaças contra a disponibilidade e a integridade, a desinformação, as ameaças não-maliciosas e os ataques contra as cadeias de fornecimento.[3] Em Portugal as ameaças são similares, no entanto o *phishing/smishing* parece ter maior presença relativa, bem como algumas formas de intrusão e diversas modalidades de fraude ou burla.[4]

III. GESTÃO DOS RISCOS A NÍVEL MACRO

Na gestão dos riscos de cibersegurança o papel do Estado é fundamental. Nos últimos anos, a generalidade dos países tem desenvolvido iniciativas para neutralizar ou minimizar os impactos das falhas de segurança cibernética, nos domínios institucional, legal, regulatório e organizacional. Portugal é um dos países que mais tem progredido nos últimos anos. De acordo com o Índice Global de Cibersegurança (GCI), publicado anualmente pela União Internacional de Telecomunicações (ITU), em 2021 Portugal surge na posição n.º 14 à escala global, depois de ter avançado quase trinta posições em três anos.[5]

A arquitetura institucional e o quadro legal de cibersegurança em Portugal são muito influenciados pelos desenvolvimentos legislativos na União Europeia. O enquadramento jurídico-institucional da União é fundamental para reforçar a cibersegurança a nível macro, proteger infraestruturas e entidades críticas, reduzir a incerteza para a generalidade dos agentes económicos e dar segurança jurídica às empresas e aos cidadãos.

O papel da União Europeia não se esgota no domínio jurídico-institucional. Recentemente, a Comissão Europeia tem lançado diversas iniciativas no domínio da cibersegurança que visam promover a inovação, potenciar o desenvolvimento de produtos e serviços europeus e aumentar a soberania estratégica, fomentar a criação e o crescimento de empresas no setor e aumentar a sua competitividade à escala global.

IV. EXPOSIÇÃO DIGITAL NAS EMPRESAS

O crescimento dos riscos cibernéticos das empresas está associado ao aumento da sua exposição digital. Nas diversas dimensões que aumentam essa exposição, nomeadamente, a ligação à Internet, a presença digital, as compras e vendas *online*, a interconexão automática com clientes e fornecedores, a adoção de sistemas de alojamento remoto, a integração de outros sistemas de operação automática/autónoma, e, mais recentemente, o forte crescimento do trabalho não presencial,[6] as empresas portuguesas estão ainda atrás das suas congéneres europeias. Embora esta situação possa ter consequências sobre a competitividade do tecido empresarial português, do ponto de vista da cibersegurança pode ser uma vantagem. A menor exposição digital das empresas nacionais pode ser aproveitada para melhorar o seu nível de cibersegurança, através de medidas, práticas e protocolos que reduzam o número de incidentes e as suas consequências.

1. Impactos sobre terceiros derivados das ações de um agente económico no desenvolvimento da sua atividade corrente.

2. *World Economic Forum* (2022).

3. ENISA (2021).

4. CNCS (2021).

5. ITU, UN (2021).

6. Especialmente através de dispositivos não corporativos.

V. GESTÃO DOS RISCOS A NÍVEL MICRO

Na gestão dos riscos cibernéticos a nível empresarial são fundamentais a adoção de medidas de cibersegurança, a formalização de protocolos de cibersegurança e a promoção da cultura de cibersegurança. Dado o aumento da exposição digital, a intensificação dos processos de digitalização e o aumento e diversificação dos volumes de dados privados geridos, as empresas devem reforçar os mecanismos de proteção, deteção e resposta dos seus sistemas. Simultaneamente, devem introduzir medidas de segurança cibernética mais sofisticadas e abrangentes e prestar maior atenção a âmbitos onde as disrupções poderão ter maiores consequências financeiras e reputacionais.

A generalidade das empresas portuguesas dispõe de alguma medida de segurança, mas definem ou reveem a sua política de segurança com pouca frequência e, regra geral, não a documentam. Genericamente, as medidas de segurança das TIC adotadas pelas empresas portuguesas são similares às das empresas europeias. No entanto, os seus empregados estão menos consciencializados que a média da União sobre as suas obrigações em matéria de cibersegurança.[7]

A proporção de empresas portuguesas que afirmam ter sofrido alguma vez problemas derivados de incidentes de segurança das TIC é muito reduzida. Os problemas resultantes dos incidentes mais frequentes, tanto em Portugal como na União Europeia, são a indisponibilidade de serviços de TIC, a destruição ou corrupção de dados e a divulgação de informação comercial.[7] Provavelmente, a reduzida incidência dos ataques explica o baixo nível de contratação de seguros contra riscos cibernéticos por parte das empresas portuguesas, se comparado com o das suas congéneres europeias.

VI. O MERCADO

A cibersegurança é um mercado em expansão, que cresce impulsionado pela explosão das ciberameaças, em geral, e do cibercrime, em particular. O mercado da cibersegurança tem crescido intensamente na última década e meia. Em 2020, o seu valor global aumentou até mais de 133 mil milhões de dólares, multiplicando por 38 o valor de 2004.[8] Os serviços de segurança constituem o principal segmento de mercado. Os que mais crescem são a segurança *cloud* e, a bastante distância, a segurança de dados.

Portugal é um dos mercados de menor dimensão da Europa. Em 2021, o valor do mercado português de cibersegurança foi de 165 milhões de euros, aproximadamente.[9] Espera-se que, nos próximos anos, o mercado português apresente elevadas taxas de crescimento anual, embora de apenas um único dígito.

B. OFERTA DE SERVIÇOS DE CIBERSEGURANÇA – RECURSOS HUMANOS E EMPRESARIAIS

I. OFERTA DE PROFISSIONAIS DE CIBERSEGURANÇA[10]

Sexo	
Masculino	84,2%
Feminino	13,9%
Idade	
30 anos ou menos	20,3%
De 31 a 40 anos	26,7%
De 41 a 50 anos	39,7%
51 anos ou mais	13,3%
Qualificação	
Doutoramento	4,2%
Licenciatura pré-Bolonha ou Mestrado	52,1%
Bacharelato ou licenciatura de Bolonha	26,7%
Não superior	17,0%

7. Eurostat.

8. Gatner (2021).

9. Baseado em diversas fontes e estimativas (IDC e Gatner).

10. Inquérito aos Profissionais de Cibersegurança, Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI).

Distribuição geográfica	
Lisboa e Vale do Tejo	58,2%
Norte	20,3%
Centro	15,5%
Alentejo e Algarve	4,5%
Ilhas	1,5%
Experiência profissional	
5 anos ou menos	42,4%
Entre 6 e 10 anos	20,3%
Entre 11 e 20 anos	27,6%
21 anos ou mais	9,7%
Sectores onde desenvolvem a sua atividade	
Serviços e produtos de telecomunicações e TI	50,0%
Administração pública e Estado	11,5%
Indústria	9,1%
Ensino, academia, investigação e desenvolvimento	7,6%
Instituições bancárias, financeiras e seguros	6,4%
Outros	15,4%
Tarefas e atividades desenvolvidas	
Auditoria de segurança	10,6%
Consultoria interna ou como prestador de serviço	10,2%
Gestão de segurança da organização	8,6%
Administração de segurança em sistemas de informação	6,1%
Formação, ensino e investigação académica	5,8%
Gestão de projetos de segurança	5,6%
Outros	53,1%
Situação face ao emprego	
Empregados por conta de outrem (sem termo ou efetivos)	83,3%
Empregados por conta de outrem (a prazo)	7,0%
Empregados por conta própria	8,8%
Desempregados	0,9%
Rendimento bruto anual	
Menos de 20 mil euros	12,8%
De 20 a 35 mil euros	30,6%
De 35 a 50 mil euros	26,9%
De 50 a 65 mil euros	16,2%
De 65 a 80 mil euros	7,3%
Mais de 80 mil euros	6,1%

II. OFERTA DE EMPRESAS DE CIBERSEGURANÇA[11]

Grupo potencial de empresas de cibersegurança	
Sectores de Consultoria e Programação Informática e Atividades Relacionadas e Atividades dos Serviços de Informação	
Empresas ativas (n.º)	5.573
Empregos totais (n.º)	67.460
Empregos médios (n.º)	12,1
Volume de negócios total (milhões de euros)	5.445
Volume de negócios médio (milhões de euros)	0,977
Grupo nuclear de empresas de cibersegurança	
Empresas que referem as atividades de Segurança Informática e diretamente relacionadas no seu objeto social ou na descrição dos produtos ou serviços	
Empresas ativas (n.º)	144
Empregos totais (n.º)	1.312
Empregos médios (n.º)	9,1
Volume de negócios total (milhões de euros)	129,9
Volume de negócios médio (milhões de euros)	0,902

As empresas do grupo potencial e do grupo nuclear têm um volume médio de ativos similar e as primeiras recorrem menos a capitais alheios. O nível médio de liquidez e de resultados é semelhante para as empresas de ambos os grupos, no entanto, o valor acrescentado é menor nas empresas do grupo nuclear.

C. PROCURA DE SERVIÇOS DE CIBERSEGURANÇA – A PROCURA DAS PEQUENAS E MÉDIAS EMPRESAS PORTUGUESAS[12]

I. EXPOSIÇÃO E RISCOS

Formas de presença digital	
E-mail corporativo	85,5%
Página de Internet	82,1%
Presença em redes sociais	63,0%
Plataformas de visibilização de negócio	20,9%
Plataformas de gestão de clientes – CRM	13,4%
Outras	19,4%
Tipos de informação processada	
Dados pessoais ou empresariais de fornecedores e clientes	74,6%
Dados bancários de empregados, fornecedores ou clientes	53,0%
Dados pessoais de empregados (incluindo dados de saúde)	42,3%
Dados de cartões de crédito	11,4%

11. Cálculos próprios a partir de dados da Base de Dados Orbis Europe.

12. Cálculos próprios a partir de dados do Inquérito às Pequenas e Médias Empresas Portuguesas sobre Cibersegurança, realizado no âmbito deste estudo.

Avaliação do potencial impacto financeiro na organização de uma possível interrupção da rede ou das TIC	
Nunca avaliaram	43,5%
Avaliaram e o impacto é significativo	29,5%
Avaliaram e o impacto é marginal	9,8%
Não sabem (ou não respondem)	17,2%
Avaliação do potencial impacto reputacional na organização de uma possível violação de dados	
Sem impacto	13,4%
Com impacto significativo	47,9%
Com impacto marginal	23,4%
Não sabem (ou não respondem)	15,3%
Avaliação do potencial impacto do incumprimento de contratos com terceiros derivado de violação de dados ou interrupção de rede	
Sem impacto	31,7%
Com impacto significativo	31,4%
Com impacto marginal	18,1%
Não sabem (ou não respondem)	18,8%

II. CIBERSEGURANÇA – RECURSOS

Orçamento de cibersegurança	
Sem orçamento	8,4%
Menos de 3.000€	36,8%
Entre 3.000€ e 8.000€	17,2%
Entre 8.001€ e 15.000€	6,9%
Entre 15.001€ e 50.000€	6,6%
Mais de 51.001€	3,4%
Não sabe (ou não responde)	20,7%
Gestão da cibersegurança	
Internamente	32,9%
Externamente	50,4%
Familiar/amigo	0,5%
Ninguém	7,6%
Não sabe (ou não responde)	8,6%
Profissionais a tempo completo na função de cibersegurança – empresas que assumem a função internamente	
Um colaborador	70,0%
Dois colaboradores	15,0%
Mais de dois colaboradores	15,0%
Principais fontes de recrutamento de profissionais de cibersegurança – empresas que assumem a função internamente	
Própria empresa – promoção interna	50,9%
Outras empresas	17,9%
Empresas de recrutamento e seleção	15,0%
Instituições de ensino	9,4%
Consultoras de cibersegurança	6,4%
Empresas de trabalho temporário	0,4%

Motivos que dificultam a contratação de profissionais de cibersegurança	
Escassez de profissionais a nível local	78,4%
Elevado custo dos profissionais	56,8%
Elevada concorrência por este tipo de profissionais	40,5%
Escassa atratividade da empresa	16,2%

A certificação dos trabalhadores em matéria de cibersegurança é marginal nas PMEs portuguesas – apenas 4,2% das empresas ou dos seus trabalhadores possuem certificações deste tipo.

III. CIBERSEGURANÇA – MEDIDAS

Medidas de cibersegurança utilizadas	
Atualização regular do *software*	86,3%
Autenticação dos utilizadores através de palavra-passe segura	77,8%
Controlo de acessos à rede da empresa	72,9%
Conservação de registos para análise posterior	34,3%
Testes de segurança às TIC	22,0%
Técnicas de cifra de dados, documentos ou *e-mails*	20,9%
Avaliação de riscos ligados às TIC	18,9%
Identificação e autenticação através de métodos biométricos	7,0%
Barreiras à melhoria dos níveis de cibersegurança	
Custo das medidas e recursos	47,1%
Escassa cultura de cibersegurança dos colaboradores	26,5%
Falta de pessoal adequado / qualificado	22,6%
Desconhecimento das medidas a adotar	22,0%
Falta de tempo / oportunidade	20,9%
Necessidade de formar os colaboradores	20,1%
Dificuldade para adquirir tecnologia	11,4%
Não sabe (ou não responde)	25,6%
Ações de formação e sensibilização em cibersegurança	
Sem ações de formação	56,9%
De 1 a 5 horas por ano	32,3%
De 6 a 10 horas por ano	5,6%
De mais de 10 horas por ano	5,1%
Auditorias de redes e sistemas	
Sem auditar	22,5%
Aditados com regularidade	38,4%
Auditados sem regularidade	22,3%
Não sabe (ou não responde)	16,8%

Em matéria de cultura de cibersegurança, as PMEs portuguesas consideram, em geral, que os seus colaboradores estão cientes da importância da cibersegurança, nomeadamente em termos de privacidade de dados e segurança, e que os planos de recuperação de incidentes são eficazes. Não obstante, as PMEs entendem que existem défices nos protocolos de atuação em caso de ciberataques e nas políticas de classificação de informação.

IV. CIBERSEGURANÇA – INCIDENTES

Frequência dos incidentes de cibersegurança	
Raramente – menos de 5 vezes por ano	78,1%
Com pouca frequência – entre 5 e 10 vezes por ano	11,0%
Com frequência – uma vez por mês ou mais	5,8%
Com muita frequência – uma vez por semana ou mais	5,2%
Principais tipologias de incidentes de cibersegurança	
SPAM	77,4%
Phishing / Smishing	59,4%
Ransomware	51,6%
Software malicioso	49,7%
Tentativas de *login* por parte de terceiros	28,4%
Exploração de vulnerabilidades	22,6%
Engenharia social	16,8%
Scanning aos sistemas da organização	16,8%

Aparentemente as empresas conhecem melhor os custos do *software* malicioso, do *Phishing / Smishing* e do SPAM, provavelmente devido à sua maior incidência/frequência. Nas tipologias de incidentes menos frequentes as empresas têm menor conhecimento dos seus impactos nos custos. As PMEs portuguesas associam o SPAM a custos mais baixos. Contrariamente, associam o *ransomware* e o *software* malicioso a custos significativos.

PMEs com seguros contra riscos cibernéticos	5,0%
Principais coberturas dos seguros contra riscos cibernéticos	
Incidentes de cibersegurança	78,1%
Responsabilidade civil derivada de violação de dados	59,4%
Danos em *software* e ***hardware***	53,1%
Proteção jurídica	53,1%

INTRODUÇÃO

As tendências dos últimos anos colocaram a Cibersegurança como uma das áreas de atenção prioritária para governos e empresas. Com a pandemia da COVID-19 e a intensificação do uso das Tecnologias de Informação e Comunicação (TIC), as questões de cibersegurança assumem uma relevância sem precedentes. A crescente interconexão entre governos, empresas e utilizadores particulares é, por um lado, uma fonte de oportunidades para a melhoria das sociedades e o aumento do bem-estar social, mas, por outro, a origem de importantes desafios, sobretudo em matéria de segurança informática.

A cibersegurança possui várias dimensões, de entre as quais, no contexto deste relatório, se destaca a económica, que se manifesta em diferentes âmbitos. À escala macroeconómica os défices de segurança e o impacto dos ciberataques podem condicionar o crescimento económico. A nível micro, os particulares podem ver o seu bem-estar notoriamente reduzido e as empresas os seus lucros significativamente comprometidos.

A omnipresença das TIC nos processos industriais, comerciais, financeiros e administrativos aumenta a exposição dos agentes económicos a potenciais incidentes de segurança informática. A deficiente operação e/ou proteção dos sistemas de TIC tem impactos negativos cada vez mais significativos sobre as atividades e operações desses agentes, que só poderão ser mitigados ou minimizados através do aumento dos níveis de proteção contra potenciais ciberataques ou incidentes de segurança de outra natureza.

Embora este relatório aborde a dimensão económica da cibersegurança, está especialmente centrado na problemática da cibersegurança nas empresas. Do lado da oferta, dimensiona e caracteriza o setor da cibersegurança em Portugal, e do lado da procura, caracteriza e analisa os níveis de exposição e as políticas, práticas e protocolos de cibersegurança nas empresas portuguesas, especialmente nas de pequena e média dimensão.

Desta forma, a principal finalidade do relatório é conhecer o estado da cibersegurança em Portugal, na dimensão económico-empresarial. Para dar cumprimento a esse desiderato são estabelecidos diversos objetivos, designadamente: i) Conhecer a relevância dos riscos cibernéticos à escala global e ao nível do país e identificar as principais tendências em matéria de cibersegurança; ii) Explicar o contexto institucional e regulatório da cibersegurança em Portugal; iii) Descrever os principais motivos explicativos do aumento dos riscos cibernéticos nas empresas e as principais políticas e práticas em matéria de cibersegurança nesse âmbito, posicionando as empresas portuguesas face às dos restantes países europeus; iv) Quantificar e qualificar a oferta de cibersegurança em Portugal, nomeadamente os recursos humanos e empresariais existentes; e, v) Caracterizar a procura de cibersegurança por parte das PMEs portuguesas.

Este documento utiliza dados secundários de diversas fontes, nomeadamente da *Eurostat*, da Base de Dados *Orbis Europe*, do *World Economic Forum* e de diversas agências internacionais ligadas à cibersegurança. Recorre ainda a informação de outros relatórios produzidos pelo Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS). Apresenta também os resultados de um inquérito realizado pela Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI), com o apoio do Observatório de Cibersegurança, sobre os profissionais do setor. A informação primária utilizada no documento procede de um inquérito destinado às PMEs do país, promovido pelo CNCS com o apoio do IAPMEI, no âmbito deste relatório.

No atual contexto e tendo em consideração a evolução no médio prazo, as empresas parecem estar cada vez mais cientes de que a cibersegurança é um investimento absolutamente imprescindível para garantir o normal funcionamento das suas operações. Apesar do crescente investimento por parte das empresas nesta área, a maior incidência do *malware* e a proliferação de ataques informáticos tem vindo a aumentar a sua perceção de insegurança.

Nesta conjuntura, os governos estão preocupados com a pertinência das políticas ligadas à cibersegurança atualmente em vigor, com a resiliência dos sistemas e infraestruturas críticos e com a capacidade do ecossistema empresarial dedicado à cibersegurança dos seus países. Desta forma, a velocidade e importância das mudanças disruptivas no sector obriga a uma monitorização permanente da sua evolução quer do lado da oferta, quer do lado da procura, utilizando indicadores que permitam o seu acompanhamento e o desenho de políticas públicas adaptadas a uma realidade em constante evolução.

O relatório integra cinco capítulos substantivos. O primeiro destina-se a analisar a relação entre economia e cibersegurança, a dimensionar os riscos cibernéticos e a identificar as principais tendências em termos de ameaças e cibersegurança. O enquadramento institucional e regulatório da cibersegurança em Portugal e na União Europeia são apresentados e discutidos no capítulo dois. No capítulo três analisa-se a problemática da cibersegurança nas empresas europeias, enquadrando a situação das organizações empresariais portuguesas. A oferta de serviços de cibersegurança e a procura desses serviços pelas empresas são caracterizadas nos capítulos quatro e cinco, respetivamente. As conclusões sintetizam alguns dos contributos do estudo, sistematizam recomendações de política e apontam áreas de exploração futura para completar o entendimento da relação entre economia e cibersegurança.

CAPÍTULO I
CIBERSEGURANÇA
ECONOMIA, RISCOS E MERCADO

CAPÍTULO I
CIBERSEGURANÇA - ECONOMIA, RISCOS E MERCADO

1.1 ENQUADRAMENTO

A cibersegurança é crítica para a prosperidade e a segurança das sociedades digitalizadas. As atividades cibernéticas maliciosas são uma ameaça para o funcionamento da economia e das democracias. A segurança futura dos países e das suas sociedades, bem como do seu tecido económico e da sua estrutura empresarial, dependem das capacidades de proteção contra as ameaças cibernéticas que consigam desenvolver.

No âmbito económico é difícil encontrar um processo industrial, comercial, financeiro administrativo ou contabilístico, entre outros, que não recorra às TIC. As atividades económicas dependem criticamente dos sistemas baseados nessas tecnologias. Desta forma, a deficiente operação ou funcionamento desses sistemas, quer por motivos acidentais, quer por motivos deliberados, impacta negativamente sobre organizações e atores económicos e, inclusivamente, sobre infraestruturas críticas, dando origem a custos significativos.

Estas circunstâncias fazem com que os cibercriminosos tentem aproveitar as vulnerabilidades desses sistemas com a finalidade de as explorar, de alguma forma, e obter assim benefícios económicos ou criar uma sensação de insegurança entre determinados grupos e organizações. Isto é particularmente frequente entre as empresas. Em 2019, 13% das empresas europeias afirmam ter experimentado, pelo menos uma vez, um incidente de segurança grave.[13,14] Em Portugal a incidência é menor, dado que apenas 8% das empresas declaram ter sofrido este tipo de incidentes. Tanto na União Europeia como em Portugal estes incidentes aumentam significativamente à medida que aumenta a dimensão da empresa.

Este capítulo debruça-se sobre a relação entre economia e cibersegurança, sobre a crescente importância dos riscos cibernéticos e sobre o mercado da cibersegurança. Na secção 1.2 explica-se a problemática do investimento em cibersegurança, as principais barreias e as medidas para mitigá-las ou eliminá-las. Na secção 1.3 evidencia-se a importância dos riscos cibernéticos, no contexto dos riscos globais, e apresenta-se um referencial para mensurar os progressos na gestão desses riscos a nível macro, assim como os *rankings* correspondentes. A secção 1.4 elenca as principais tendências no domínio das ciberameaças e da cibersegurança. A dimensão e evolução do mercado de cibersegurança discutem-se na secção 1.5.

1.2 ECONOMIA E CIBERSEGURANÇA

A cibersegurança tem vindo a ganhar a atenção dos responsáveis de política pública. Uma parte significativa dos problemas de cibersegurança tem caráter económico. A sua resolução pode passar, em muitos casos, por intervenções que alinhem incentivos ou corrijam falhas de mercado. Em muitas ocasiões, os sistemas falham porque as organizações que os protegem não suportam a totalidade dos custos dessas falhas. As medidas de política e a legislação em geral devem ter como finalidade melhorar a atribuição de responsabilidades, para que os agentes envolvidos, com capacidade de resolução de problemas, tenham incentivos para o fazer.

O grande crescimento dos incidentes de segurança, em geral, e dos ciberataques, em particular, é, em grande medida, explicado por um conjunto de barreiras de natureza económica que impedem que o investimento em cibersegurança alcance níveis eficientes. As principais barreias são: i) os incentivos desalinhados; ii) as assimetrias de informação; e, iii) as externalidades.[15]

A falta de alinhamento dos incentivos entre os que devem responsabilizar-se pela segurança e os que beneficiam da proteção são uma característica dos sistemas de TIC. Os sistemas de informação têm maior propensão a falhar quando a pessoa ou a empresa responsável pela proteção não é quem sofre as consequências quando as falhas ocorrem. Em muitas ocasiões, no âmbito destes sistemas os riscos são deficientemente alocados.

No domínio da informação, existem incentivos para reportar menos incidentes dos que efetivamente ocorrem. Por exemplo, empresas de certos sectores tendem a não revelar as perdas por fraude por motivos de credibilidade junto dos seus clientes; noutros casos, as empresas minimizam a sua cooperação com a polícia, na sequência de incidentes de segurança, em geral, e de ciberespionagem, em particular, porque têm consequências em termos de reputação; os operadores de infraestruturas críticas e de serviços essenciais podem ter receio de tornar pública informação sobre os ataques que sofrem, por medo de que as potenciais vulnerabilidades sejam conhecidas.

13. Algumas afirmam ter experimentado mais de um.

14. Eurostat.

15. Impactos sobre terceiros derivados das ações de um agente económico no desenvolvimento da sua atividade corrente.

Esta falta de informação precisa faz com que a sociedade não invista no tipo de defesas mais adequadas para lutar contra os incidentes e, se o fizer, que o faça abaixo do nível eficiente. Os consumidores e as empresas mal informadas tendem a investir em soluções de má qualidade se não possuírem um bom conhecimento das ameaças e das defesas. Simultaneamente, as empresas de *software* nem sempre disponibilizam no mercado soluções de segurança que protejam os agentes económicos contra as ameaças mais significativas. Para resolver esses problemas é fundamental investir em medidas que reduzam a assimetria de informação, disponibilizando informação confiável aos diferentes *stakeholders* envolvidos, quer do lado da oferta, quer do lado da procura.

O sector das TIC é caracterizado pela existência de externalidades, ou seja, de situações onde as ações de um dado agente têm consequências sobre terceiros. No âmbito da segurança das TIC manifestam-se múltiplas tipologias de externalidades, nomeadamente, externalidades de rede, externalidades de insegurança e a denominada segurança interdependente.

As externalidades de rede estão vinculadas à elevada concentração do setor das TIC, em geral, e do da produção de *software*, em particular. Estas externalidades manifestam-se quando as escolhas dos agentes económicos dependem tanto das características e desempenho dum produto ou de uma plataforma como do tamanho da rede, ou seja, do número de pessoas/empresas que fez a mesma escolha previamente. No caso dos protocolos de Internet, a existência de externalidades de rede também explica o falhanço de muitas atualizações seguras, dado que os benefícios que delas derivam não se materializam até que um elevado número de utilizadores as adotem.

A insegurança gera externalidades negativas. Um computador infetado ligado a uma rede pode provocar danos nos sistemas de outros utilizadores para além do infetado. Os custos sociais derivados de falhas de segurança nos sistemas são maiores que os custos individuais das mesmas. Dado que os riscos privados que enfrentam as empresas são menores que os riscos sociais é expetável que o nível de investimento em proteção contra riscos cibernéticos seja inferior ao eficiente.

A segurança interdependente está relacionada com os investimentos em segurança. Estes podem ser estrategicamente complementares: um indivíduo que invista em medidas de proteção cria externalidades positivas noutros, no entanto, por sua vez, pode criar desincentivos a que esses outros invistam. Ou seja, os investimentos de determinados agentes dependem da perceção que tenham sobre os investimentos realizados pelos restantes agentes.[16]

Para limitar os impactos dessas barreiras ao investimento em cibersegurança podem ser adotadas diferentes intervenções regulatórias. A primeira é a regulação da segurança *ex ante* e a responsabilização *ex post*. A regulação da segurança ***ex ante*** está concebida para evitar incidentes mediante prescrição de medidas preventivas antes da sua ocorrência. Nesta solução, as empresas adotam políticas de segurança e boas práticas e testam o seu cumprimento das regras.

Uma alternativa à regulação *ex ante* proactiva consiste em responsabilizar *ex post* à parte responsável pela falha.[17] A racionalidade desta abordagem é que a ameaça de que se produzam danos monetários derivados de ações legais incentive os agentes a tomar as precauções necessárias, para minimizar a probabilidade de ocorrência de falhas de segurança.

A segunda tipologia de intervenção é a divulgação de informação. Dado que as assimetrias de informação são uma barreira fundamental para melhorar os níveis de cibersegurança, afigura-se fundamental melhorar a disponibilização de informação. A divulgação de informação é uma potente ferramenta para reduzir as assimetrias de informação e ajustar incentivos desajustados.

Os seguros são outro dos mecanismos para gerir os riscos derivados da segurança da informação e das configurações em rede. Estes instrumentos podem gerar fortes incentivos para que os indivíduos e as organizações adotem as medidas de segurança mais adequadas em cada caso. Um mercado robusto de ciberseguros pode dar origem a benefícios significativos para a sociedade. Em primeiro lugar, as companhias de seguros podem retribuir os investimentos em segurança, reduzindo os prémios para os agentes mais avessos ao risco. Em segundo lugar, dado que as companhias de seguros baseiam a sua vantagem competitiva na diferenciação dos prémios ajustada pelos níveis de risco, as seguradoras têm incentivos para recolher dados sobre incidentes de segurança, quando são reportados para efeitos de ativação dos seguros. Desta forma, os ciberseguros são frequentemente apontados como uma solução para os desafios informacionais que condicionam os investimentos em cibersegurança. Por último, tal como noutras modalidades de seguros, os ciberseguros podem contribuir para que as empresas suavizem os seus resultados financeiros, dado que ao contratar um seguro deste tipo estão a trocar um custo presente de montante relativamente reduzido e de caráter fixo, o prémio do seguro, por perdas futuras potencialmente elevadas e de caráter incerto.

16. Varian, H. (2004), System Reliability and Free Riding, in Jean Camp, L. e S. Lewis (Eds.), *Economics of Information Security*. Advances in Information Security Series, vol. 12. Springer, pp. 1-15.

17. Em Portugal esta possibilidade está contemplada na Lei 46/2018, de 13 de agosto, e no Decreto-Lei 65/2021, de 30 de julho.

O último tipo de intervenção é a denominada "responsabilização indireta do intermediário". Nos regimes de responsabilidade indireta, determinados agentes, nomeadamente os intermediários, podem ser responsabilizados pelas ações de terceiros. No contexto da cibersegurança, os agentes que podem detetar ou evitar ações perniciosas e internalizar[18] as externalidades próprias das transações digitais e que, portanto, podem ser alvo de responsabilização indireta, são os Fornecedores de Serviços de Internet (ISPs).

Os regimes de responsabilização indireta são aplicados sobretudo em duas circunstâncias[19]: i) quando os causantes do dano estão fora do alcance da lei, porque não podem ser identificados ou porque, mesmo que fossem identificados e condenados, não poderiam assumir o custo dos danos provocados; e, ii) quando devido aos elevados custos de transação não for viável desenhar corretamente os contratos que distribuem as responsabilidades entre as partes. Existem ainda outros dois fatores que contribuem para justificar a utilização da responsabilização indireta: i) se determinados agentes (neste caso, os intermediários) estiverem numa posição favorável para detetar ou evitar ações perniciosas; e, ii) se determinados agentes (neste caso, os intermediários), não envolvidos diretamente na transação, estiverem em condições de assumir as consequências dos impactos negativos[20], reduzindo os impactos das ações perniciosas.

A configuração do mercado da cibersegurança condiciona a tipologia das transações e as formas de relação entre os agentes participantes. Nesse mercado, a existência de grandes fornecedores de serviços e de grandes operadores restringe os níveis de concorrência. Nessas circunstâncias, o poder de mercado dos utilizadores é praticamente nulo e, portanto, não dispõem de qualquer capacidade negocial.

Neste contexto, os custos das falhas de segurança ou das atividades ilícitas são maioritariamente suportados pelos utilizadores, sem que os impactos sobre os produtores tenham implicações, em termos de custos, em linha com os seus níveis de responsabilidade. No mercado de cibersegurança verificam-se fortes assimetrias de informação entre a oferta e a procura. Os fornecedores não conhecem o alcance real da segurança do *software* e os compradores não estão dispostos a pagar um preço adicional pelo *software*, porque não têm informação suficiente sobre o seu nível de segurança.[21] As empresas de desenvolvimento de *software* têm escassos incentivos para melhorar a segurança do *software*, dado que o custo das falhas de segurança que suportam pode ser muito reduzido. Contrariamente, o custo individual para os utilizadores e, em termos agregados, o custo social dessas falhas pode ser extremamente elevado.

Neste mercado existem também problemas relacionados com a sua configuração em rede. Estando as partes integradas numa rede, quando alguns agentes realizam investimentos em segurança com impactos sobre a segurança da rede, outros, nomeadamente os que possuem menores níveis de segurança, passam a ter menores incentivos para melhorar a sua própria segurança. Estes efeitos-rede tendem a piorar a alocação de riscos nos contextos digitais e geram incentivos perversos entre os diferentes intervenientes.

1.3 RISCOS GLOBAIS E RISCOS CIBERNÉTICOS

1.3.1. A VISÃO GLOBAL

Não obstante as inquestionáveis vantagens da transformação digital, esta está também associada a novos riscos derivados da adoção de novas TIC. O crescimento dos riscos derivados das ameaças à segurança da informação está vinculado:

- Ao maior impacto dos ataques à segurança da informação, devido à generalização da adoção das TIC como elementos centrais nos processos de negócio;
- À maior probabilidade de ocorrência dos ataques, devido à maior abrangência das tecnologias utilizadas. Adicionalmente, a sofisticação e a inovação tecnológica contribuem para aumentar os impactos dos ciberataques individualmente;
- Ao aumento das vulnerabilidades derivado da adoção crescente de novos modelos de trabalho remoto, com recurso a dispositivos próprios dos trabalhadores, não abrangidos pelos sistemas e políticas de segurança da organização e eventualmente comprometidos;
- À expansão do cibercrime e ao aumento das suas possibilidades de monetização, que acabam por atrair a um número de crescente de organizações criminais dedicadas também a outros negócios ilícitos.

O último relatório de *Riscos Globais* do World Economic Forum (WEF, 2022)[22] inclui as falhas de cibersegurança entre os principais riscos suscetíveis de constituir uma ameaça para o mundo. No horizonte de riscos globais, as falhas de cibersegurança são o 7º risco mais relevante a curto prazo (até 2 anos), por constituírem um perigo claro e atual, e o 8º mais relevante a médio prazo (3 a 5 anos), pelo seu potencial para produzir efeitos em cadeia (Tabela 1.1). Os *scores* deste risco são especialmente elevados nos países desenvolvidos. Entre os riscos potencialmente mais severos no longo prazo (5 a 10 anos) não aparece nenhum risco tecnológico.

18. Assumir as consequências.

19. Lichtman D. e E. Posner (2006), Holding internet service providers accountable, in M. Grady and F. Parisi (Eds.), *The Law and Economics of Cybersecurity*, Cambridge University Press, pp. 221-258.

20. Internalizar as externalidades negativas.

21. Fonfría A. e N. Duch-Brown (2020), Ciberseguridad Económica. RIEC ARI 105/2020. Real Instituto Elcano, Madrid.

22. WEF (2022) (Disponível em: https://www.weforum.org/reports/the-global-risks-report-2022).

Tabela 1.1 – Horizonte de riscos globais 2022

RK	Principais riscos c/p (0-2 anos)	RK	Principais riscos m/p (2-5 anos)
1	Climatologia extrema (A)	1	Falhas na ação climática (A)
2	Crises nos meios de vida (S)	2	Climatologia extrema (A)
3	Falhas na ação climática (A)	3	Erosão da coesão social (S)
4	Erosão da coesão social (S)	4	Crises nos meios de vida (S)
5	Doenças infeciosas (S)	5	Crises de dívida (E)
6	Deterioração da saúde mental (S)	6	Dano ambiental humano (A)
7	Falhas de cibersegurança (T)	7	Confrontações geoeconómicas (G)
8	Crises de dívida (E)	8	Falhas de cibersegurança (T)
9	Desigualdade Digital (T)	9	Perda de Biodiversidade (A)
10	Explosão de bolhas mercados ativos (E)	10	Explosão de bolhas mercados ativos (E)
Notas:	Categorias de risco		
	E – Económico	A – Ambiental	G – Geopolítico
	S – Social	T – Tecnológico	

Fonte: *The Global Risks Report 2022*, World Economic Forum

Tabela 1.2 – Horizonte de riscos globais 2021

RK	Principais riscos c/p (0-2 anos)	RK	Principais riscos m/p (2-5 anos)
1	Doenças infeciosas (S)	1	Explosão de bolhas mercados ativos (E)
2	Crises nos meios de vida (S)	2	Falhas na infraestrutura IT (T)
3	Eventos climatológicos extremos (A)	3	Instabilidade de preços (E)
4	Falhas de cibersegurança (T)	4	*Shocks* nas commodities (E)
5	Desigualdade digital (T)	5	Crises de dívida (E)
6	Estagnação permanente (E)	6	Quebras nas relações entre estados (G)
7	Ataques terroristas (G)	7	Conflitos entre estados (G)
8	Descontentamento jovem (S)	8	Falhas de cibersegurança (T)
9	Erosão da coesão social (S)	9	Falhas de governança tecnológica (T)
10	Dano ambiental humano (A)	10	Geopolitização dos recursos (G)
Notas:	Categorias de risco		
	E – Económico	A – Ambiental	G – Geopolítico
	S – Social	T – Tecnológico	

Fonte: *The Global Risks Report 2021*, World Economic Forum

A rápida globalização nas economias avançadas durante a pandemia da Covid-19 deu origem a novas vulnerabilidades cibernéticas. As falhas de cibersegurança foram um dos riscos que mais pioraram desde o início da pandemia da Covid-19. Concretamente foi o 7º risco que mais se agravou, logo atrás de (por esta ordem): a erosão da coesão social, as crises de meios de vida, as falhas na ação climática, a deterioração da saúde mental, a climatologia extrema e as crises de dívida.

No relatório de 2021 (WEF, 2021),[23] as falhas de cibersegurança surgiam no horizonte de riscos globais como o 4º risco mais relevante a curto prazo (até 2 anos) e como o 8º mais relevante a médio prazo (3 a 5 anos) (Tabela 1.2). No médio prazo também surgia em 2º lugar um risco que pode estar diretamente relacionado com as falhas de segurança, designadamente as falhas nas infraestruturas IT. Neste prazo, outra falha de natureza tecnológica, as falhas de governança tecnológica aparecem em 8º lugar. A longo prazo (5 a 10 anos), os avanços tecnológicos adversos, também de natureza tecnológica, constituem o 4º risco de maior relevância no ranking referente a ameaças existenciais.

23. WEF (2021) (Disponível em: https://www.weforum.org/reports/the-global-risks-report-2021).

No mesmo relatório de 2021 os riscos associados às falhas de cibersegurança integram o top-10 das categorias de risco por probabilidade, nomeadamente na nona posição. Nos relatórios de Riscos Globais de anos anteriores (2017, 2018, 2019 e 2020), no top-5 dos riscos por probabilidade apareceram sempre riscos relacionados com a cibersegurança. Nos de 2020 e 2019, as fraudes com dados e os ciberataques apareceram em 4º e 5º lugares, respetivamente. No de 2018, os ciberataques surgiram em 3º lugar e as fraudes com dados em 4º. No de 2017, as fraudes com dados foram consideradas o 5º risco mais relevante em termos de probabilidade de ocorrência.

1.3.2. A VISÃO PORTUGUESA

A Marsh[24] elabora desde há vários anos um relatório sobre a visão das empresas portuguesas em matéria de riscos. Na sétima edição, de 2021,[25] as empresas portuguesas consideram que o principal risco que o mundo irá enfrentar são as pandemias/propagação rápida de doenças infeciosas. Após três edições (2018, 2019 e 2020) sendo para as empresas portuguesas os principais riscos a nível global, os riscos cibernéticos passam a ser a segunda tipologia de risco mais relevante.[26] A Tabela 1.3 apresenta os principais riscos globais, de acordo com as empresas portuguesas, quer em 2020, quer em 2021.

Tabela 1.3 – Principais riscos globais 2020 e 2021

RK	2020	RK	2021
1	Ataques cibernéticos em grande escala (T)	1	Pandemia/propagação rápida de doenças infeciosas (S)
2	Eventos climáticos extremos (A)	2	Ataques cibernéticos em grande escala (T)
3	Crimes fiscais e financeiros em economias chave (E)	3	Crimes fiscais e financeiros em economias chave (E)
4	Ataques terroristas em larga escala (G)	4	Elevado desemprego ou subemprego estrutural (E)
5	Instabilidade social profundas (S)	5	Falta de governance nacional (G)
		5	Eventos climáticos extremos (A)

Notas:	Categorias de risco		
	E – Económico	A – Ambiental	G – Geopolítico
	S – Social	T – Tecnológico	

Fonte: A visão das empresas portuguesas sobre os riscos 2020 e 2021, Marsh.

Na Tabela 1.4 apresentam-se os principais riscos para as empresas, segundo as empresas portuguesas, em 2020 e 2021. Em ambos os exercícios, tal como nos dois anos precedentes, os ataques cibernéticos são considerados pelas empresas o principal dos vários riscos que enfrentam. Em 2021, a pandemia e o surgimento de eventuais surtos epidémicos ou pandémicos situam-se em 2º lugar no *ranking* dos principais riscos para as empresas portuguesas. Com o mesmo *score* aparece também a instabilidade política e social, que, em certa medida, é também consequência da pandemia.

Curiosamente, ao contrário do que acontece no relatório de *Riscos Globais* do WEF, os riscos ambientais têm menor relevância para as empresas portuguesas. As entidades empresariais em Portugal outorgam maior ponderação aos riscos de natureza económica e social, tais como a instabilidade política e social, as crises económicas e sociais, os problemas do mercado de trabalho ou as configurações das estruturas de mercado.

24. Pertencente ao grupo Marsh McLennan, que é uma empresa líder mundial de serviços profissionais nas áreas de risco, estratégia e capital humano. É uma das empresas parceiras, conjuntamente com o *Zurich Insurance Group*, do *World Economic Forum* para a elaboração do Global Risks Report.

25. Marsh (2021) (Disponível em: https://www.marsh.com/pt/pt/risks/global-risk/insights/a-visao-das-empresas-portuguesas-sobre-os-riscos-2021.html).

26. Marsh (2020) (Disponível em: https://www.marsh.com/pt/pt/risks/global-risk/insights/a-visao-das-empresas-portuguesas-sobre-os-riscos-2020.html).

Tabela 1.4 – Principais Riscos para as Empresas 2020 e 2021			
RK	2020	RK	2021
1	Ataques cibernéticos (T)	1	Ataques cibernéticos (T)
2	Retenção de talentos (E)	2	Pandemia/surtos (S)
3	Instabilidade política ou social (S)	2	Instabilidade política ou social (S)
4	Eventos climáticos extremos (A)	3	Recessão (E)
5	Concorrência (E)	4	Eventos climáticos extremos (A)
		5	Crises financeiras/crises fiscais (E)
Notas:	Categorias de risco		
	E – Económico	A – Ambiental	G – Geopolítico
	S – Social	T – Tecnológico	
Fonte: A visão das empresas portuguesas sobre os riscos 2020 e 2021, Marsh.			

Segundo a Marsh, as empresas portuguesas dão uma importância crescente à gestão de riscos: 48% das empresas portuguesas confere uma importância elevada à gestão de riscos (face a 35% em 2017). O incremento da relevância outorgada a esta matéria traduz-se num aumento dos recursos alocados a este fim. No mesmo estudo, 33% dos respondentes indicam que o orçamento destinado à gestão de riscos aumentou em 2021.

1.3.3. A GESTÃO DE RISCOS A NÍVEL MACRO

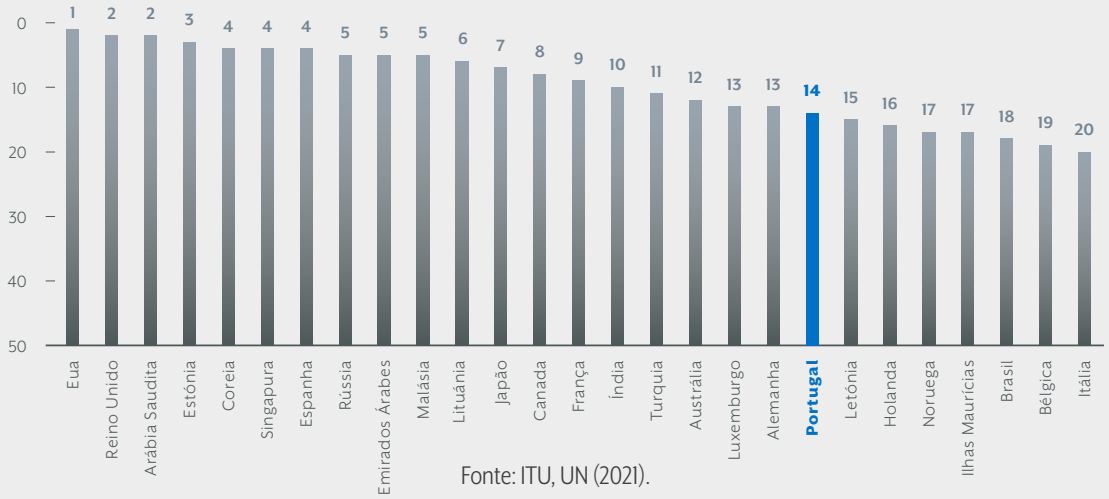
Lidar com as tipologias de riscos que a cibersegurança tenciona mitigar exige um forte compromisso das sociedades e das organizações, mas sobretudo dos governos. Há países que nos últimos quinze anos têm desenvolvido iniciativas para neutralizar ou minimizar os impactos das falhas de segurança cibernética, incluindo o cibercrime, nos domínios institucional, legal, regulatório e organizacional.

Com a finalidade de medir os avanços nas medidas adotadas pelos países para melhorar os níveis de cibersegurança, a União Internacional de Telecomunicações (ITU), que é a agência especializada em TIC das Nações Unidas, publica anualmente o *Índice Global de Cibersegurança* (GCI).[27] Este exercício anual, iniciado em 2015, pretende identificar áreas de melhoria e incentivar os países a desenvolver estratégias no domínio da cibersegurança, através da identificação e publicitação do estado da cibersegurança à escala global. O Índice Global de Cibersegurança sintetiza a situação dos países em cinco pilares/dimensões, com impactos sobre os níveis de cibersegurança: i) Medidas legais; ii) Medidas técnicas; iii) Medidas organizacionais; iv) Medidas cooperativas; e, v) Desenvolvimento de Capacidades.

27. ITU, UN (2021) (Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf).

O *ranking* com as vinte primeiras posições entre os países avaliados na edição de 2020 do *Índice Global de Cibersegurança* constam da Figura 1.1. Na Figura 1.2 apresentam-se os *scores* correspondentes a esses países. O país líder em matéria de cibersegurança à escala global é os Estados Unidos, seguido do Reino Unido e da Arábia Saudita. Os países que integram os vinte primeiros lugares no *ranking* são muito heterogéneos. Constam economias desenvolvidas, tais como os Estados Unidos, o Reino Unido, o Canadá, a Austrália, o Japão, a Coreia do Sul e as grandes economias da UE, assim como os países Bálticos, grandes economias em desenvolvimento, tais como a Rússia, a Índia, a Turquia e o Brasil, economias de rápido crescimento da Ásia, como a Singapura e a Malásia, e ainda economias do Golfo Pérsico, tais como a Arábia Saudita e Emirados Árabes Unidos.

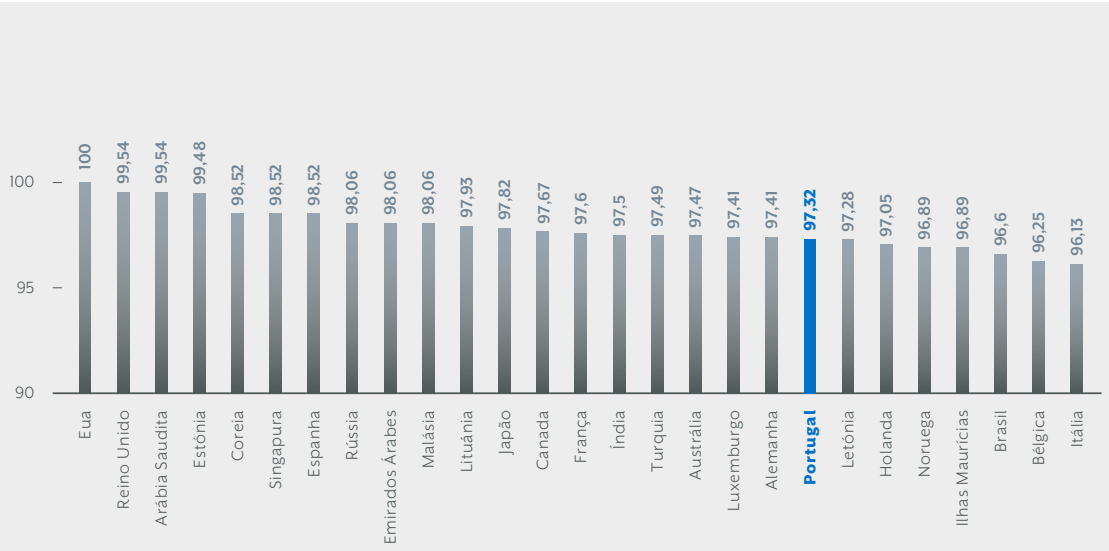
Figura 1.1 – *Ranking* do *Índice Global de Cibersegurança* | Top 20 – Edição de 2020



Fonte: ITU, UN (2021).

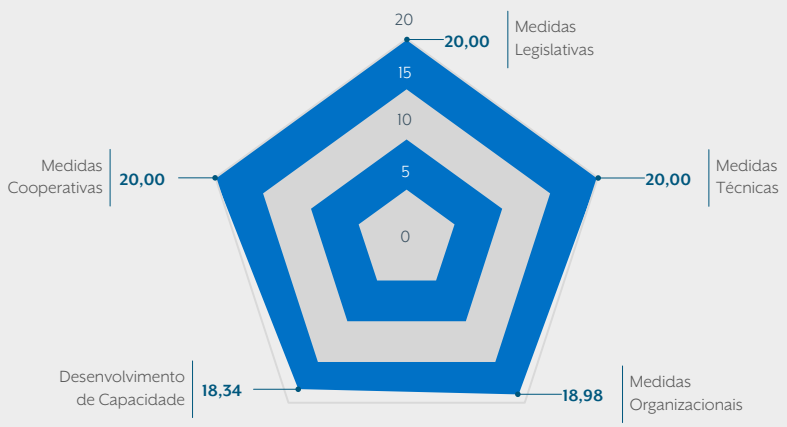
Em 2021, Portugal ocupa a posição nº 14 no *ranking* do *Índice Global de Cibersegurança*. Nos últimos anos, os progressos efetuados pelo país nas várias dimensões utilizadas para o seu cálculo permitiram um forte avanço no índice e consequentemente no *ranking*, passando da posição 42º, na Edição de 2018, para a referida 14º posição, na Edição de 2021. O *score* de Portugal nos cinco pilares que constituem o índice consta da Figura 1.3.

Figura 1.2 – *Scores* do *Ranking* do *Índice Global de Cibersegurança* | Top 20 – Edição de 2020



Fonte: ITU, UN (2021).

Figura 1.3 – *Scores* do nos cinco pilares do *Índice Global de Cibersegurança* – Portugal



Fonte: ITU, UN (2021).

Não obstante o bom desempenho do país no *Índice Global de Cibersegurança*, existe ainda alguma margem de melhoria, nomeadamente nos domínios das medidas organizacionais e do desenvolvimento de capacidade. Nos restantes domínios os progressos dos últimos anos permitiram ao país obter as pontuações máximas.

1.4. AS TENDÊNCIAS: CIBERAMEAÇAS E CIBERSEGURANÇA

No último relatório anual sobre ciberameaças da ENISA, a Agência de Cibersegurança da União Europeia, são identificadas como principais ameaças cibernéticas (ENISA, 2021):[28]

- O *ransomware*
- O *malware*
- O *cryptojacking*
- As ameaças ligadas ao correio eletrónico
- As ameaças vinculadas a dados
- As ameaças contra a disponibilidade e a integridade
- A desinformação digital
- As ameaças não-maliciosas
- Os ataques contra as cadeias de fornecimento

A nível nacional, segundo o relatório de ***Riscos e Conflitos*** do Observatório de Cibersegurança as principais ciberameaças são (CNCS, 2021):[29]

- O *phishing/smishing*
- O *malware*
- O *ransomware*
- Algumas formas de intrusão
- Variados tipos de fraude / burla
- A *sextortion*
- A desinformação digital

O relatório evidencia, em 2020, um aumento significativo no volume de incidentes de cibersegurança e dos indicadores de cibercrime. Simultaneamente, identifica os cibercriminosos e os agentes estatais como os principais agentes de ameaças no ciberespaço de interesse nacional.

28. ENISA (2021) (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021).

29. CNCS (2021)) (Disponível em: https://www.cncs.gov.pt/docs/relatorio- riscos-confli tos2021-observatoriociberseguranca-cncs.pdf).

No período de reporte (abril 2020 a julho de 2021), o relatório da ENISA identifica as seguintes tendências gerais em matéria de cibersegurança (ENISA, 2021):

i. O *ransomware* constitui atualmente a principal ameaça;
ii. A obtenção de retorno financeiro passou a ser uma das principais motivações dos cibercriminosos, daí o auge do *ransomware*. As criptomoedas continuam a ser o principal método de pagamento para os cibercriminosos;
iii. O crescente volume de infeções com recurso a *criptojacking* – devido às motivações financeiras referidas;
iv. A perda de importância do *malware*;
v. A alteração das características das campanhas de DDoS (*Distributed Denial of Services*), que são cada vez mais personalizadas, persistentes e multivector; a *Internet of Things* (IoT) e as redes móveis são os principais alvos das novas vagas de ataques DDoS;
vi. O aumento dos incidentes não-maliciosos;
vii. A crescente concentração de ataques no setor da saúde, nomeadamente de violação de dados;
viii. A continuidade da utilização da Covid-19 como principal isco para iniciar os ataques;
ix. O aumento da mobilização dos governos para enfrentar as ciberameaças, quer a nível nacional, que a nível internacional;
x. O crescente uso de linguagens de programação pouco conhecidas para desenvolver os códigos de determinadas tipologias de ataques.

Em Portugal, o referido relatório de *Riscos e Conflitos* do CNCS sumaria as seguintes tendências gerais em matéria de cibersegurança (CNCS, 2021):

i. O aumento da perceção de risco de se sofrer um incidente de cibersegurança no ciberespaço de interesse nacional;
ii. O incremento da perceção de capacitação do ciberespaço de interesse nacional – ou pelo menos a manutenção da perceção de capacitação;
iii. A persistência das ciberameaças emergentes e dos agentes de ameaças, graças à existência de um contexto favorável. Para além das ciberameaças mais frequentes, é expectável que ocorram ataques oportunistas ao trabalho remoto, às cadeias de fornecimento, aos setores da banca e da saúde e às tecnologias emergentes.

O aumento do número dos ciberataques e da gravidade das suas consequências supõem custos crescentes para as empresas. No caso dos ciberataques sem motivações económicas, os prejuízos derivam dos danos nos sistemas, das perdas de informação, dos impactos na reputação e, sobretudo, da interrupção temporária desses sistemas, com consequências sobre a operação e o negócio no seu conjunto.

No caso dos ciberataques com motivações económicas, para além dos prejuízos referidos, as empresas têm que assumir custos adicionais, nomeadamente quando existem resgates para liberar sistemas ou repor informação sensível. Para além desses custos, as empresas veem-se confrontadas com a dificuldade para efetuar o pagamento dos resgates, normalmente em criptomoedas, e com hesitações na hora de os registar quer a nível contabilístico, quer a nível fiscal. Nestes ciberataques com motivações económicas, os cibercrimosos obtêm retornos significativos por via do resgate ou pela venda de informação sensível com interesse para terceiros (processos industriais, tecnologia, historiais médicos, etc.).

Perante o aumento dos ciberataques e dos seus impactos sobre as suas contas, as empresas devem delinear estratégias e políticas de cibersegurança, que evitem incidentes e minimizem as suas consequências. Com base nas principais tendências em matéria de cibersegurança nas empresas, identificadas por algumas das principais consultoras internacionais,[30] as políticas de cibersegurança no meio empresarial podem sistematizar-se nos seguintes termos:

i. O fortalecimento dos sistemas de proteção, deteção e resposta para elevar a segurança da *cloud*, dada a intensificação do seu uso – pelas suas vantagens num contexto laboral cada vez mais descentralizado e distribuído;
ii. O aumento da importância da gestão da identidade e dos processos de autenticação, dada a crescente necessidade de aceder aos sistemas empresariais a partir de localizações externas às empresas. Neste âmbito, prevê-se que ganhem importância abordagens baseadas em *Zero trust* (confiança zero) e *Passwordless* (segurança sem palavras-passe), bem como a autenticação multifactor;

30. Kaspersky (2021) (Disponível em: https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends); Deloitte (2021) (Disponível em: https://www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf); EY (2021) (Disponível em: ey-wgs-security-by-design 2021%20(2).pdf).

iii. A intensificação do recurso a técnicas avançadas de cifra e ao *blockchain* para garantir a integridade dos dados e reforçar a segurança, especialmente em transações financeiras, compras *online* e comunicações pessoa a pessoa;
iv. O reforço da segurança nas cadeias de fornecimento, para evitar disrupções que afetem a operação de cadeias completas, com impactos significativos sobre as contas de resultados das empresas;
v. A utilização de novas formas de proteção, identificação e resposta baseadas na Inteligência Artificial (IA), na automatização e em *Machine Learning*, para preservar a operação de plataformas e sistemas assentes tanto em tecnologias maduras como em novas tecnologias, tais como a *Internet of Things* (IoT) ou o 5G;
vi. A adoção de tecnologias e a implementação de controlos para gerir as ameaças do *ransomware*, que continua a crescer e é cada vez mais frequente e custoso, e da engenharia social, que cresce exponencialmente, graças ao uso de IA para suplantar identidades mediante o *deepfake*;
vii. Os esforços de adaptação às novas regulações em matéria de segurança,[31] de privacidade de dados pessoais e de comportamento das pessoas no ciberespaço (pegada digital), assim como a contratação de delegados de proteção de dados, dada a necessidade de cumprir com um quadro normativo cada vez mais amplo e exigente;
viii. O entendimento crescente da cibersegurança como um serviço. Dada a falta de recursos e a sofisticação das ameaças, as empresas estão a migrar para um modelo de gestão de riscos de cibersegurança assente na externalização, que lhes permite centrar-se no seu negócio.

1.5. O MERCADO DA CIBERSEGURANÇA

A cibersegurança é um mercado em expansão, que cresce impulsionado pela explosão das ciberameaças, em geral, e do cibercrime, em particular. Os investimentos das organizações em tecnologia têm que ser acompanhados de investimentos em segurança, para evitar que os riscos associados à sua utilização impactem negativamente sobre os benefícios esperados.

O mercado da cibersegurança tem um caráter estratégico. Dispor de capacidades para o desenvolvimento de produtos e tecnologias de cibersegurança, para proteger os sistemas de TIC e as infraestruturas críticas e os serviços essenciais, permite melhorar a soberania dos países neste domínio. A redução da dependência exterior é um objetivo para áreas integradas como a União Europeia, que atualmente está fortemente dependente das empresas americanas do sector.

Por esse motivo, é fundamental desenvolver capacidades no domínio da cibersegurança, apostando na inovação e na diferenciação. Este vetor de desenvolvimento é central num mercado em que os ciberataques crescem em sofisticação, graças à inovação subjacente. Inovar na área da cibersegurança é uma condição *sine qua non* para garantir proteção face aos riscos associados às novas ameaças.

A cibersegurança é também uma oportunidade de negócio para as empresas. As perspetivas de crescimento do mercado criam espaço para o aparecimento de novas empresas num sector dominado por empresas americanas, embora existam *players* relevantes à escala global em países como a Rússia ou Israel. Inclusivamente, do ponto de vista macroeconómico, desenvolver localmente uma indústria de cibersegurança poderá ter impactos muito positivos sobre o emprego, o rendimento e a balança comercial do país em questão.

O mercado da cibersegurança tem crescido intensamente na última década e meia. Em 2004, o mercado global de cibersegurança valia à volta de 3.500 milhões de dólares. Em 2020, o seu valor aumentou até mais de 133 mil milhões de dólares, multiplicando por 38 o valor de 2004. Na Tabela 1.5 constam os valores da despesa global em cibersegurança, por segmento, nos últimos cinco anos (2017-2021). Nesse período, a despesa neste domínio aumentou cerca de 50 mil milhões de dólares, com um crescimento acumulado superior a 48%.[32] O crescimento anual continua a ser robusto, dado que em 2021 atingiu os 12,4%.

Em 2021, os serviços de segurança foram a principal categoria de despesa, tendo atingido os 72,5 mil milhões de dólares à escala global. Os segmentos de mercado que mais crescem são a segurança *cloud* (41,2%) e, a uma distância considerável, a segurança de dados (17,5%).

Contrariamente a outros sectores tecnológicos cujo crescimento é impulsionado pela redução de ineficiências e o aumento da produtividade, a despesa em cibersegurança é, em grande medida, ativada pelo aumento dos riscos e dos ciberataques. Dada a dificuldade para antecipar o crescimento dos ciberataques, é também muito difícil prever o crescimento da despesa em cibersegurança, embora seja previsível que o seu ritmo de crescimento se acelere ainda mais nos próximos anos. As previsões indicam que o mercado de cibersegurança mais que duplicará até 2026, atingindo nesse ano os 352,25 mil milhões de dólares.[33] Desta forma, o crescimento anual no período 2020-2026 será de 14,5%, aproximadamente.

31. No caso português, ao Regime Jurídico da Segurança do Ciberespaço (Lei 46/2018, de 13 de agosto).

32. Gatner (2021) (Disponível em: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem).

33. Research and Markets (2021) (Disponível em: https://www.researchandmarkets.com/reports/4591630/cyber-security-market-growth-trends-covid-19).

Tabela 1.5 – Despesa global em Cibersegurança por segmento, 2017-2021, Milhões de dólares				
Segmento de Mercado	2017	2020	2021	Δ 20-21 (%)
Segurança de Aplicações	2.432	3.333	3.738	12,2
Segurança na Nuvem	185	595	841	41,2
Segurança dos Dados	2.563	2.981	3.505	17,5
Gestão da Identidade de Acessos	8.823	12.036	13.917	15,6
Proteção de Infraestruturas	12.583	20.462	23.903	16,8
Gestão Integrada do Risco	3.949	4.859	5.473	12,6
Equipamentos de Redes de Segurança	10.911	15.626	17.020	8,9
Outro *Software* de Segurança da Informação	1.832	2.306	2.527	9,6
Serviços de Segurança	52.315	65.070	72.497	11,4
Software de Segurança dos Consumidores	5.948	6.507	6.990	7,4
Total	101.544	133.776	150.409	12,4
Notas	Nota: Devido aos arredondamentos, a soma de alguns valores pode não ser igual aos totais. Alguns valores podem não ser exatamente iguais aos reais, dado que, em alguns casos, são estimações – as diferenças não deveriam ser significativas.			
Fonte: Gartner (2021).				

Na Europa os principais mercados de cibersegurança são o Reino Unido e a Alemanha, seguidos de Holanda, França, Espanha, Polónia e Itália. Portugal é um dos mercados de menor dimensão no continente Europeu. Com base em dados da IDC, estima-se que, em 2021, o valor do mercado de cibersegurança em Portugal seja de 165 milhões de euros, aproximadamente, e que continue a crescer a taxas anuais próximas de 7%.[34,35]

34. As estimativas mais recentes sobre o mercado da cibersegurança em Portugal são da IDC. Segundo esta consultora, o mercado português valia, em 2018, 135,97 milhões de euros e situava o crescimento anual do mercado entre 2018 e 2022 em 6,71%.

35. IDC (2020) (Disponível em: https://www.idcdx.pt/insights/insights-up/uploads/2020/09/idc_360_pt.pdf).

DESTAQUES CAPÍTULO I

Uma parte significativa dos problemas de cibersegurança tem caráter económico. O grande crescimento dos incidentes de segurança é, em grande medida, explicado por um conjunto de barreiras de natureza económica, que impedem que o investimento em cibersegurança alcance níveis eficientes. A falta de alinhamento dos incentivos, as assimetrias de informação e a existência de externalidades são as três principais barreiras que limitam o investimento em segurança cibernética.

Para limitar os impactos dessas barreiras ao investimento podem ser adotadas diferentes medidas regulatórias: i) A regulação da segurança *ex ante* e a responsabilização *ex post*; ii) A divulgação de informação para reduzir assimetrias; iii) Os seguros contra riscos cibernéticos; e, iv) A responsabilização indireta do intermediário.

O crescimento dos riscos derivados das ameaças à segurança da informação está vinculado ao maior impacto dos ataques e à sua maior probabilidade de ocorrência. Os riscos associados às falhas de cibersegurança integram o Top-10 das categorias de risco, por probabilidade, incluídos nos últimos relatórios de *Riscos Globais* do World Economic Forum.

No horizonte de riscos globais incluído no relatório de 2022, as falhas de cibersegurança são o 7º risco mais relevante a curto prazo (até 2 anos), por constituírem um perigo claro e atual, e o 8º mais relevante a médio prazo (3 a 5 anos), pelo seu potencial para produzir efeitos em cadeia.

De acordo com os últimos relatórios da Marsh, para as empresas portuguesas os ataques cibernéticos são o principal dos vários riscos que enfrentam. As empresas nacionais dão uma importância cada vez maior à gestão de riscos e, simultaneamente, alocam recursos crescentes a esta finalidade.

Na gestão dos riscos de cibersegurança o papel dos governos é fundamental. Nos últimos anos, diversos países do mundo têm desenvolvido iniciativas para neutralizar ou minimizar os impactos das falhas de segurança cibernética, nos domínios institucional, legal, regulatório e organizacional. Para medir esses progressos, a União Internacional de Telecomunicações (ITU), integrada nas Nações Unidas, publica anualmente o Índice Global de Cibersegurança (GCI).

De acordo com o GCI, em 2021, o país líder em cibersegurança à escala global é os Estados Unidos, seguido do Reino Unido e da Arábia Saudita. Portugal, que em 2018 ocupava a posição n.º 42 no *ranking*, graças aos progressos realizados nos últimos anos, surge em 2021 na posição nº 14.

Segundo a ENISA, atualmente as principais ameaças cibernéticas são: o *ransomware*, o *malware*, o *cryptojacking*, as ameaças ligadas ao correio eletrónico, as ameaças vinculadas a dados, as ameaças contra a disponibilidade e a integridade, a desinformação, as ameaças não-maliciosas e os ataques contra as cadeias de fornecimento. Para a mesma agência, em termos gerais, as principais tendências em cibersegurança são: i) a consolidação do *ransomware* como principal ameaça; ii) o aumento das motivações financeiras dos cibercriminosos; iii) o aumento do recurso a *criptojacking*; iv) a perda de importância do *malware*; v) a alteração das características das campanhas de DDoS (*Distributed Denial of Services*); vi) o aumento dos incidentes não-maliciosos; vii) A crescente concentração de ataques no setor da saúde; viii) a continuidade da utilização da Covid-19 como principal isco para iniciar os ataques; ix) o aumento da mobilização dos governos para enfrentar as ciberameaças; e, x) o crescente uso nos ataques de linguagens de programação pouco convencionais.

As políticas de cibersegurança no meio empresarial destinam-se essencialmente a: i) o fortalecimento dos sistemas de proteção, deteção e resposta para elevar a segurança da *cloud*; ii) o aumento da importância da gestão da identidade e dos processos de autenticação; iii) a intensificação do recurso a técnicas avançadas de cifra e ao *blockchain* para garantir a integridade dos dados e reforçar a segurança; iv) o reforço da segurança nas cadeias de fornecimento; v) a utilização de novas formas de proteção, identificação e resposta baseadas na IA, na automatização e em *Machine Learning*; vi) a adoção de tecnologias e controlos para gerir as ameaças do *ransomware* e da engenharia social; vii) o aumento da preocupação com a privacidade de dados pessoais e do comportamento das pessoas no ciberespaço; e, viii) o entendimento crescente da cibersegurança como um serviço.

A cibersegurança é um mercado em expansão, que cresce impulsionado pela explosão das ciberameaças, em geral, e do cibercrime, em particular. O mercado da cibersegurança tem crescido intensamente na última década e meia. Em 2020, o seu valor aumentou até mais de 133 mil milhões de dólares, multiplicando por 38 o valor de 2004.

Em 2021, a despesa em cibersegurança ultrapassou os 150 mil milhões de dólares. Os serviços de segurança foram a principal categoria de despesa, tendo atingido os 72,5 mil milhões de dólares à escala global. Os segmentos de mercado que mais crescem são a segurança *cloud* (41,2%) e, a uma distância considerável, a segurança de dados (17,5%). Prevê-se que em 2026, o mercado de cibersegurança ultrapasse os 352,25 mil milhões de dólares.

Portugal é um dos mercados de menor dimensão da Europa. Estima-se que, em 2021, o valor do mercado de cibersegurança em Portugal seja de 165 milhões de euros, aproximadamente, e que, no curto prazo, continue a crescer a taxas anuais próximas de 7%.

CAPÍTULO II
ENQUADRAMENTO REGULATÓRIO DA CIBERSEGURANÇA EM PORTUGAL
FONTES, EVOLUÇÃO E SITUAÇÃO ATUAL

CAPÍTULO II
ENQUADRAMENTO REGULATÓRIO DA CIBERSEGURANÇA EM PORTUGAL – FONTES, EVOLUÇÃO E SITUAÇÃO ATUAL

2.1 ENQUADRAMENTO

Neste capítulo são apresentados o enquadramento institucional e normativo e a arquitetura sectorial da Cibersegurança em Portugal. Do ponto de vista económico, estes aspetos são de extrema importância para reforçar a cibersegurança a nível macro, reduzir a incerteza para a generalidade dos agentes económicos e dar segurança jurídica às empresas e aos cidadãos.

Dada a grande importância que a União Europeia tem tido, e continua a ter, na construção do quadro legal e institucional do país em matéria de cibersegurança, na secção 2.2 é apresentada a evolução do edifício regulamentar, da organização institucional e da estratégia, bem como das perspetivas da União Europeia no domínio da segurança do ciberespaço. A seguir expõe-se a situação em Portugal, dando especial ênfase à arquitetura institucional da cibersegurança no país. Por último, na secção 2.4, apresenta-se e discute-se a atividade das principais instituições internacionais em matéria de cibersegurança, pela influência que estas têm na emissão de orientações, recomendações e boas práticas, no estabelecimento de *standards*, na capacitação de agentes e entidades e no intercâmbio internacional.

2.2 A UNIÃO EUROPEIA

O primeiro documento estratégico sobre cibersegurança na União Europeia, intitulado *Estratégia de Cibersegurança na União Europeia: um ciberespaço aberto, seguro e protegido*, foi publicado em 2013.[36] Nele, a Comissão atribuía aos governos um papel central em matéria de prevenção e resposta aos ciberataques, numa abordagem muito diferente da atual em que preconiza a cooperação internacional e a colaboração com o setor privado no âmbito da cibersegurança. No entanto, nessa primeira aproximação estratégica à cibersegurança, previa-se que a União Europeia pudesse ter um papel relevante em caso de um ciberataque ou ciberincidente sistémico de grandes dimensões.

Do ponto de vista económico, esta mudança de perspetiva é extremamente relevante, ao reconhecer que as instituições públicas não conseguem isoladamente fazer face aos desafios atuais da cibersegurança. A Comissão Europeia assume, deste modo, que a capacidade dos agentes privados, nomeadamente das empresas, é fundamental para detetar, analisar e construir soluções para lidar com os riscos cibernéticos. O potencial de inovação das empresas para desenvolver sistemas, dispositivos, programas e outros tipos de ferramentas que dissuadam ou bloqueiem os ciberataques ou minimizem os ciber-riscos e as suas consequências afigura-se fundamental.

A peça fundamental da arquitetura da cibersegurança na União Europeia é a Diretiva sobre a Segurança de Redes e Sistemas de Informação (Diretiva SRI), publicada em 2016.[37] Este diploma é a primeira medida legislativa à escala da União para reforçar a cooperação entre os Estados-membros em matéria de cibersegurança.[38] Nesta Diretiva foram estabelecidas obrigações de segurança para os operadores de serviços essenciais – em setores críticos como a energia, os transportes, a banca, as infraestruturas do mercado financeiro, a saúde, o fornecimento e distribuição de água potável e infraestruturas digitais – e os prestadores de serviços digitais – mercados *online*, motores de pesquisa *online* e serviços de computação na nuvem.

Os principais objetivos da Diretiva SRI são: i) criar uma cultura de segurança em sectores críticos de atividade e na sociedade no seu todo; ii) aumentar a capacidade em matéria de cibersegurança a nível nacional, obrigando os Estados-membros a dispor de uma Estratégia Nacional de Cibersegurança, de Equipas Nacionais de Resposta a Emergências (CSIRTs), de Autoridades Competentes Nacionais de Redes e Sistemas de Informação e de Pontos de Contacto Único; e, iii) melhorar a cooperação e a partilha de informação a nível comunitário mediante a criação da Rede de CSIRTs e do Grupo de Cooperação de Redes e Sistemas de Informação.

A relevância económica da Diretiva SRI está associada à sua preocupação com a segurança e a continuidade de operação de sistemas e infraestruturas críticos para o funcionamento de qualquer economia, e à construção de uma arquitetura institucional de cibersegurança a nível dos Estados-membros, que ao definir um quadro de capacidades, estratégias e respostas operacionais, reduz os níveis de incerteza associados aos riscos do ciberespaço. Por último, a componente da Diretiva associada ao aumento dos níveis de informação à disposição dos agentes públicos e privados, graças aos mecanismos de partilha estabelecidos, permite melhorar a tomada de decisões e desenhar instrumentos mais eficazes para minimizar riscos cibernéticos e o impacto dos incidentes.

36. No domínio digital, o ponto de partida para toda a produção legislativa posterior foi o Plano de Ação para a Sociedade da Informação, adotado em 1994.

37. Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho.

38. Não obstante, em muita da legislação europeia em matérias relacionadas, tal como o tratamento de dados pessoais, a assinatura eletrónica, o comércio eletrónico, as comunicações eletrónicas e inclusivamente o cibercrime, estiveram presentes preocupações com a cibersergurança.

Em setembro de 2017, a Comissão aprovou o Pacote de Cibersegurança, que revia a estratégia de 2013 e que tinha como principal finalidade proteger os cidadãos e as empresas, nomeadamente em matéria de propriedade intelectual e dados pessoais. Para além dos instrumentos já existentes, o novo pacote propôs um conjunto de iniciativas para melhorar a denominada ciberresiliência. O Pacote de Cibersegurança incluía também a denominada *Cibersecurity Act.*

Posteriormente, em dezembro de 2018, o Parlamento Europeu, o Conselho e a Comissão Europeia alcançaram um acordo político sobre a *Cibersecurity Act*, que reforça o papel da Agência de Cibersegurança da UE (ENISA), criada em 2004. Simultaneamente, a *Cibersecurity Act* estabelece um quadro europeu para a certificação em matéria de cibersegurança de serviços *online* e aparelhos eletrónicos.

Em maio de 2019, o Conselho estabeleceu um quadro que permite à União Europeia impor sanções específicas para impedir os ciberataques, que constituam uma ameaça externa para a União ou os seus Estados-membros e, inclusivamente, responder a essas agressões. Esta iniciativa permite impor sanções às pessoas ou entidades responsáveis por ciberataques ou tentativas de ciberataques, e às que prestam apoio técnico, material ou financeiro ou estejam de algum modo envolvidas – inclusivamente, a pessoas e entidades a elas associadas. Entre outras medidas contemplam-se a proibição de entrada na União Europeia, em caso de pessoas naturais, ou a imobilização de ativos quer no caso de pessoas naturais, quer no caso de entidades. As primeiras sanções por ciberataques foram impostas em julho de 2020.

A introdução de elementos dissuasórios é uma estratégia fundamental para reduzir o número de ciberataques e as suas consequências. Do ponto de vista económico, trata-se de desincentivar (através de incentivos negativos) as práticas ilegais no ciberespaço, e eliminar a sensação de impunidade que imperava entre os cibercriminosos.

Em julho de 2019 foi aprovado o Regulamento relativo à ENISA e à certificação da cibersegurança das TIC,[39] na sequência do acordo sobre a *Cibersecurity Act*. O Regulamento renova e reforça o mandado da ENISA, nas suas funções de apoio aos Estados-membros, às instituições da União e a outras entidades interessadas no combate aos ciberataques. O Regulamento introduz também um quadro europeu para a certificação em matéria de cibersegurança para produtos, processos e serviços digitais, válido em toda a União Europeia. Este referencial de certificação, que é um elemento fundamental do Mercado Único Digital, está baseado na utilização de *standards* internacionais relevantes à escala global. Este quadro de certificação surge para gerar confiança, acelerar o crescimento do mercado da cibersegurança e facilitar o comércio na União Europeia. O regulamento incluiu ainda uma iniciativa de resposta rápida a emergências, no caso de ciberacidentes ou crises transfronteiriças em grande escala, e o reforço das relações externas, especialmente com países terceiros.

O conteúdo económico do Regulamento é muito relevante. Por um lado, reforça uma entidade que combate os ciberataques, muitos dos quais com impactos financeiros muito significativos. Por outro, cria mecanismos de certificação que promovem a confiança dos consumidores e, consequentemente, contribuem para garantir a qualidade dos produtos e serviços de cibersegurança na União Europeia e alavancam o crescimento do mercado desses produtos e serviços.

Estes *standards* definem as regras que balizam o desenvolvimento de produtos e serviços de cibersegurança no âmbito comunitário, reforçando os níveis de segurança jurídica do investimento das empresas do setor e as garantias para as empresas que adquirem este tipo de produtos e serviços. Estes desenvolvimentos legislativos procuram igualmente potenciar o crescimento das empresas europeias do sector da cibersegurança e afins e melhorar a sua competitividade à escala global. Procuram também garantir que os produtos e serviços desta natureza, provenientes de mercados externos à União, cumpram requisitos congéneres, fomentando, desta forma, o aumento da resiliência geral deste mercado.

Em dezembro de 2020 a Comissão Europeia aprovou um pacote de medidas destinadas a adaptar o quadro europeu de cibersegurança à transformação induzida pelo processo de digitalização. Entre essas medidas destacam-se: i) a Estratégia de Cibersegurança da União Europeia para a Década Digital; ii) uma proposta de revisão da Diretiva de Segurança de Redes e Sistemas de informação (SRI 2.0), que substitua a de 2016; iii) uma proposta de Diretiva sobre Resiliência de Entidades Críticas, que substitua a Diretiva de Proteção de Infraestruturas Críticas (PIC), de 2008;[40] e, iv) a inclusão da cibersegurança nos fundos *Repair* e *Prepare* do pacote *Next Generation*.

Perante a aceleração do processo de digitalização e a intensificação das ameaças cibernéticas, a abordagem adaptativa da Comissão foi, provavelmente, a mais eficiente. O desajustamento entre o conteúdo dos diplomas legais e a estratégia da União, por um lado, e a realidade do mercado e das ciberameaças, por outro, teria importantes consequências económicas para as empresas em geral e para

39. Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho.

40. Diretiva (UE) 2008/114 do Parlamento Europeu e do Conselho.

as entidades críticas. O financiamento de iniciativas vinculadas à cibersegurança através dos fundos *Next Generation* é facilmente justificável, dado que os recursos destinados à recuperação pós-pandémica têm como finalidade única promover a transformação estrutural da economia Europeia, algo que não é possível sem melhorar os instrumentos e os níveis de cibersegurança.

A Estratégia de Cibersegurança da União Europeia, à qual estão associados investimentos de 4.500 milhões de euros, durante os próximos sete anos, tem como finalidade reforçar a resiliência das quatro cibercomunidades da União Europeia – o mercado, a diplomacia, a segurança e a defesa. Esta estratégia de Cibersegurança inclui um conjunto de iniciativas estratégicas, entre as quais se destacam:

i. Um ciberescudo à escala da União Europeia, integrado por centros de operações de segurança, que utilizem IA e aprendizagem automática para detetar indícios precoces de ciberataques iminentes e permitir, desse modo, adotar medidas que evitem ou minimizem os danos;
ii. Uma ciberunidade conjunta que integrará todas as comunidades de cibersegurança e que servirá para partilhar as respetivas perceções das ameaças e reagir coletivamente;
iii. Soluções europeias destinadas a reforçar a segurança da Internet à escala mundial;
iv. Um regulamento sobre segurança da Internet das Coisas (IoT);
v. Instrumentos de ciberdiplomacia mais sólidos a nível da União Europeia para prevenir, dissuadir e responder aos ciberataques;
vi. Um reforço da cooperação em matéria de cibersegurança, nomeadamente graças à revisão do Quadro Estratégico da União Europeia para a Ciberdefesa;
vii. Um programa de ação das Nações Unidas para gerir a segurança internacional no ciberespaço;
viii. Diálogos sobre cibersegurança mais frequentes e robustos com os países terceiros e as organizações regionais e internacionais, incluindo a NATO;
ix. Um programa de melhoria das capacidades cibernéticas externas da União Europeia e um comité interinstitucional da União Europeia para o reforço das capacidades cibernéticas.

No âmbito económico, os dois aspetos mais relevantes da Estratégia de Cibersegurança da União são: i) o desenvolvimento de soluções em diversos âmbitos – ciberdefesa, segurança da Internet, etc.; e, ii) o regulamento sobre segurança da IoT. O primeiro, para além dos objetivos em matéria de segurança e proteção, procura promover a investigação, o desenvolvimento e a inovação em cibersegurança ou segurança das TIC, a fim de potenciar um *cluster* sectorial à escala europeia e aumentar a soberania da União Europeia nestes âmbitos. O regulamento de segurança da IoT é de extrema relevância para potenciar a adoção desta tecnologia na União e garantir que as interconexões entre os sistemas e dispositivos ligados à Internet são suficientemente seguras.

Entre outros motivos, a aceleração da transformação digital induzida pela pandemia obrigou a Comissão a propor uma revisão da Diretiva SRI, que permitisse também dar resposta à evolução das ameaças cibernéticas. Este instrumento legislativo integra a Estratégia de Cibersegurança da União Europeia para a década digital. A revisão deste instrumento legislativo destina-se a: i) reforçar as obrigações de segurança das empresas; ii) melhorar a segurança das cadeias de fornecimento; iii) introduzir medidas de supervisão mais estritas para as autoridades nacionais, juntamente com coimas por incumprimento de normas; e, iv) intensificar as trocas de informação e a cooperação.[41]

Do ponto de vista económico, a nova Diretiva aprofunda a regulação da cibersegurança nas empresas e em estruturas supra-empresariais, direta ou indiretamente, através dos supervisores nacionais. Trata-se de preencher lacunas em matéria de regulação, evitar que comportamentos privados tenham impactos sistémicos e melhorar a segurança e a confiança dos operadores.

Um dos aspetos mais destacados da Diretiva é que alarga a regulação a novos sectores e novos serviços, para além dos contemplados na primeira versão. Desta forma, passam a ser abrangidos pela nova Diretiva, por serem considerados essenciais ou importantes, o sector alimentar, o setor espacial, os serviços digitais (ex. plataformas de serviços e centros de dados), os serviços postais e dos correios, a produção de produtos críticos (ex. equipamentos farmacêuticos e médicos), a gestão de águas residuais e resíduos, os prestadores de redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público e a administração pública. Nesta revisão, que está atualmente a ser debatida pelo Conselho, as entidades estarão sujeitas ao cumprimento da norma em função da sua importância para o funcionamento da sociedade e da economia digitais, e não em função do seu tamanho ou tipologia.

41. Para além desta proposta legislativa, a União Europeia está a trabalhar numa nova Diretiva sobre a resiliência das entidades críticas.

O impacto da pandemia no processo de transformação digital também espoletou o processo de revisão da Diretiva de Proteção de Infraestruturas Críticas. Esta revisão, que dará origem à denominada Diretiva sobre Resiliência de Entidades Críticas, aumenta o seu

âmbito de aplicação, que passa de dois a dez setores e, simultaneamente, alarga a sua abrangência funcional, ao substituir as infraestruturas críticas por entidades críticas. Estas últimas definem-se em função do impacto que a sua interrupção provoque na economia ou na vida diária dos cidadãos. Tal como a Diretiva SRI, encontra-se atualmente a ser debatida pelo Conselho.

O aumento da abrangência sectorial e do âmbito de aplicação destas Diretivas justifica-se pela necessária adaptação do quadro legal à nova realidade do mercado e à evolução das ameaças. A nova regulação tem como finalidade melhorar a eficiência dos mercados, evitando disrupções provocadas por incidentes, através da adoção de medidas que aumentem os níveis de segurança contra os principais riscos cibernéticos.

As iniciativas da Comissão Europeia não se esgotam no pacote aprovado em finais de 2020. Para 2021 e os anos seguintes, a Comissão aprovou uma agenda que inclui, entre outras, as seguintes iniciativas: i) a implementação de medidas relativas à cibersegurança de redes 5G (*EU Toolkit Box*); ii) a criação da Unidade Conjunta de Cibersegurança (*Joint Cyber Unit*) para a coordenação operacional dos Estados-membros;[42] iii) a definição de referenciais de certificação (*EU Cybersecutity Act*); iv) a regulação do acesso a comunicações cifradas para compatibilizar a privacidade e a interceção legal de comunicações; v) a revisão da Diretiva de Privacidade Eletrónica, sobre privacidade e confidencialidade das comunicações eletrónicas; e, vi) a aceleração do investimento no período 2021-2027, através dos programas Europa Digital e Horizonte Europa e do Plano de Recuperação para a Europa.

Todas estas iniciativas têm implicações económicas muito significativas, nomeadamente pelo seu impulso à inovação, à certificação de produtos e serviços e ao desenvolvimento empresarial no setor da cibersegurança. A disponibilidade de recursos, através dos programas supracitados, para financiar investimentos em cibersegurança, tanto na esfera pública como na privada, constitui uma oportunidade para o desenvolvimento setorial na União Europeia e para o reforço funcional das empresas europeias neste domínio.

Em março de 2021, o Conselho adotou um conjunto de Conclusões sobre a Estratégia de Cibersegurança, nas quais sublinha a importância da cibersegurança[43] para o futuro da Europa. Entende-se que, para dispor de autonomia estratégica, é fundamental aumentar a capacidade para adotar decisões autónomas no âmbito da cibersegurança, a fim de alcançar a liderança digital e reforçar as capacidades estratégicas da União Europeia.

Para além da legislação sobre cibersegurança, a União Europeia tem desenvolvido vários diplomas relacionados com a segurança e a privacidade dos dados. Em primeiro lugar, o Regulamento Geral sobre a Proteção de Dados,[44] em vigor desde meados de 2018, que fornece um conjunto de regras que permitem aos cidadãos ter maior controlo sobre os seus dados pessoais e confere uma vantagem competitiva aos negócios cumpridores. Em segundo lugar, a Diretiva de Privacidade Eletrónica, que garante a confidencialidade das comunicações e define as regras de rastreio e monitorização *online*. Esta Diretiva, em vigor desde 2002, será, como referido, objeto de atualização para adaptar a legislação aos novos desenvolvimentos tecnológicos e de mercado. Por último, a Regulamentação do eIDAS – Sistema de Identificação e Autenticação Eletrónica à escala Europeia,[45] que entrou em vigor em finais de 2018. Este sistema introduz diversos métodos para que os particulares e as empresas possam realizar as suas transações eletrónicas de forma segura e confiável.

Para reforçar o ecossistema de cibersegurança da União Europeia, nos últimos anos têm vindo a desenvolver-se diversas iniciativas em vários âmbitos, nomeadamente:

i. A criação de uma Rede de Centros Nacionais de Coordenação de Cibersegurança destinada a identificar áreas de Investigação e Desenvolvimento prioritárias na União Europeia;
ii. Associada à rede, a constituição, em dezembro de 2020, de um Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança[46] destinado a reunir, partilhar e disponibilizar conhecimento, apoiar o desenvolvimento de produtos e soluções de cibersegurança, partilhar investimentos em infraestruturas com custos elevados e garantir uma cooperação estratégica a longo prazo entre a indústria, as comunidades de investigação e os governos. O regulamento de criação do Centro e da Rede foi aprovado pelo Conselho em abril de 2021;[47]
iii. A formalização de uma parceria público-privada (PPP) entre a Comissão Europeia e a Organização Europeia de Cibersegurança (ECSO), que aglutina a indústria europeia de cibersegurança. Esta iniciativa, lançada em 2016, é fundamental para estruturar e coordenar os recursos industriais de segurança digital na Europa. Esta PPP inclui PMEs inovadoras, produtores de componentes e equipamentos, operadores de serviços essenciais e centros de investigação. Até 2020, esta parceria alavancou investimentos na área de cibersegurança de 1.800 milhões de euros, aproximadamente. A União Europeia comprometeu-se a investir até 450 milhões de euros nesta iniciativa, através do seu programa de investigação e inovação Horizonte Europa, sempre que a indústria invista o triplo nas mesmas áreas;

42. Já em funcionamento, que, entre outras, tem como finalidade impulsionar, em certos âmbitos, o Plano de Resposta Coordenada a Incidentes de Cibersegurança. Este Plano de Resposta tem como finalidade definir uma taxonomia de incidentes de cibersegurança, estabelecer procedimentos de resposta transnacionais e, em geral, promover a cooperação entre Estados-membros para responder a este tipo de incidentes.

43. Conselho da União Europeia (2021) (Disponível em: https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf).

44. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho.

45. Regulamento (EU) 2014/910 do Parlamento Europeu e do Conselho.

46. COM (2018) 630

47. Regulamento (UE) 2021/887 do Parlamento Europeu e do Conselho.

iv. O reforço da proteção das infraestruturas críticas da União Europeia. No âmbito das redes 5G, a União alcançou um acordo sobre um conjunto de instrumentos e medidas comuns para diminuir os principais riscos de cibersegurança nas redes 5G. No que se refere aos dispositivos conectados, que integram a IoT, o Conselho adotou, em dezembro de 2020, um conjunto de conclusões que, tendo em consideração os riscos do novo contexto em matéria de privacidade, segurança da informação e cibersegurança, estabelecem uma série de prioridades para melhorar a segurança e proteção destes dispositivos.[48]

v. O investimento em investigação, desenvolvimento e inovação de capacidades de cibersegurança, quer com recurso aos fundos do Quadro Financeiro Plurianual, quer com recurso aos programas extraordinários de recuperação.[49] A Comissão considera que se trata de investimentos estratégicos, ao permitir o reforço da base industrial e tecnológica da cibersegurança europeia e a articulação dos ecossistemas europeus que integrem a cibersegurança no desenvolvimento e implementação de novas tecnologias associadas à economia digital;

vi. O financiamento de projetos de investigação, desenvolvimento e inovação na área da cibersegurança, através do programa Horizonte Europa. No próximo período de programação, a União Europeia destinará um montante significativo de recursos a impulsionar a inovação em sistemas de cibersegurança e privacidade.[50] Para além de fomentar avanços em investigação e inovação, estes projetos dedicar-se-ão também a apoiar a colaboração transnacional e intergovernamental, a promover a partilha de conhecimento e a fornecer *inputs* para a definição de políticas públicas a nível europeu;

vii. O investimento de 1.600 milhões de euros, no âmbito do Programa Europa Digital, em capacidades de cibersegurança e no desenvolvimento geral de infraestruturas e ferramentas de cibersegurança em toda a União Europeia. Este investimento, para o período 2021-2027, destina-se a administrações públicas, empresas e particulares.

viii. A promoção de um modelo de criação de capacidades baseado em direitos, alinhado com a abordagem do *Digital4Development*.[51] As prioridades neste domínio abrangem quer a vizinhança da União, quer países em desenvolvimento cuja conectividade cresce exponencialmente. Estas iniciativas da União Europeia estão alinhadas e complementam a Agenda 2030 para o Desenvolvimento Sustentável e os programas de desenvolvimento de capacidades institucionais da União.

ix. A criação de um Centro Europeu de Cibercriminalidade (EC3), no âmbito da Europol, em 2013, para ajudar os países da União Europeia a investigar os crimes cibernéticos e combater as redes criminosas. Neste domínio destaca-se também a Plataforma Multidisciplinar Europeia contras as Ameaças Criminosas (EMPACT), que é uma iniciativa de segurança promovida pelos Estados-membros para detetar, priorizar e neutralizar as ameaças do crime organizado internacional. No âmbito económico, esta iniciativa pode ter um papel central no combate a determinadas tipologias de ataques às empresas, como por exemplo o *ransomware*. O impacto deste tipo de ataques nas empresas tem aumentado sistematicamente nos últimos dois anos.

x. A adoção em 2017 do Quadro de Resposta Diplomática Conjunta da União às Atividades Cibernéticas Maliciosas, no âmbito da denominada diplomacia cibernética da União Europeia. Este referencial estabelece as medidas de Política Exterior e Segurança Comum, constituindo um avanço importante no desenvolvimento das orientações e das capacidades de resposta a nível da União e dos Estados-membros. A União Europeia está a promover o estabelecimento de um quadro estratégico para a resolução de conflitos e a estabilidade no ciberespaço no contexto dos seus acordos bilaterais, regionais e multilaterais. Neste domínio, a União promove a aplicação do direito internacional, nomeadamente da Carta das Nações Unidas, ao ciberespaço.

A grande dinâmica das instituições europeias no âmbito da segurança do ciberespaço está a impulsar a europeização da cibersegurança, nomeadamente pelo crescente protagonismo da Comissão, da ENISA e dos órgãos de gestão de crises. Neste contexto observa-se também um aumento da relevância dos atores privados, nomeadamente de caráter coletivo, no desenvolvimento da soberania digital em detrimento dos Estados-membros.

48.Conselho da União Europeia (2020) (Disponível em: https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf).

49. Segundo a Comissão, os investimentos no conjunto da cadeia de fornecimento em tecnologias digitais deveriam representar no mínimo 20% (134,5 mil milhões de euros) dos fundos do Mecanismo de Recuperação e Resiliência, que tem uma dotação de 672,5 mil milhões de euros para empréstimos e subvenções.

50. As soluções europeias em matéria de ciberdefesa serão financiadas pelo Fundo Europeu de Defesa (FED).

51. Comissão Europeia (2017) (Disponível em: https://futurium.ec.europa.eu/en/Digital-4Development/library/digital4development--mainstreaming-digital-technologies-and-services--eu-development-policy).

2.3. PORTUGAL

Em Portugal, as políticas públicas e os instrumentos legislativos no domínio da cibersegurança estão alinhados com as orientações da União Europeia.[52] A primeira iniciativa com alguma expressão relacionada com a cibersegurança, em Portugal, foi a aprovação em 2009 da Lei n.º 109, de 15 de setembro, de Cibercrime, destinada a aumentar a segurança dos cidadãos no ciberespaço e a conferir instrumentos de intervenção às entidades que combatem o cibercrime. Esta lei resulta da transposição da Decisão-Quadro 2005/222/JAI, do Conselho, sobre ataques contra os sistemas de informação, e adaptou à legislação nacional a Convenção de Budapest sobre Cibercrime, de 23 novembro de 2001.

Em 2011, foi aprovado o Decreto-Lei n.º 62/2011, de 9 de maio, que estabelece os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social nos setores da energia e dos transportes. Esta legislação transpôs para o ordenamento jurídico português a Diretiva de Proteção de Infraestruturas Críticas (PIC), que igualmente tem como finalidade identificar e proteger essas infraestruturas a nível europeu.

Em 2012, para implementar e consolidar uma Estratégia Nacional de Segurança da Informação, o governo decidiu criar o Centro Nacional de Cibersegurança, através da Resolução do Conselho de Ministros n.º 12/2012, de 7 de fevereiro. A responsabilidade pela constituição da comissão instaladora do novo centro foi atribuída ao Gabinete Nacional de Segurança.[53] Posteriormente, em 2014, foram definidas as características, competências e regime de funcionamento do Centro Nacional de Cibersegurança, através do Decreto-Lei n.º 69, de 9 de maio.

Em 2013, o governo, no âmbito da revisão do Conceito Estratégico de Defesa Nacional,[54] define um conjunto de prioridades em matéria de proteção contra o Cibercrime e o Ciberterrorismo, nomeadamente:

- Garantir a proteção das infraestruturas de informação críticas;
- Definir uma Estratégia Nacional de Cibersegurança;
- Criar uma estrutura responsável pela Cibersegurança;
- Sensibilizar os operadores sobre o caráter crítico da segurança da informação;
- Aumentar a capacidade de Ciberdefesa.

Em 2015 foi aprovada a Estratégia Nacional de Segurança do Ciberespaço, através da Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho. Esta estratégia visa estabelecer, de acordo com as orientações gerais da Estratégia da União Europeia para a Cibersegurança, objetivos e linhas de ação para melhorar a gestão das crises, a coordenação das repostas aos ciberataques, o desenvolvimento de sinergias nacionais, e a cooperação nacional, internacional e europeia. Os objetivos estratégicos desta iniciativa eram:

- Organizar a segurança do ciberespaço;
- Combater o cibercrime;
- Proteger o ciberespaço e as infraestruturas nacionais;
- Promover a educação, a consciencialização e a prevenção;
- Incentivar a investigação e desenvolvimento; e,
- Promover a cooperação.

Na sequência da aprovação dessa Estratégia, é proposto que o Centro Nacional de Cibersegurança assuma, progressivamente, funções de coordenação operacional e de autoridade nacional em matéria de cibersegurança, no entanto, esse mandado apenas é consolidado com a aprovação do Regime Jurídico da Segurança do Ciberespaço em 2018. A Estratégia Nacional de Segurança do Ciberespaço prevê também que o Centro Nacional de Cibersegurança possa apoiar o desenvolvimento de capacidades de reação a incidentes, através da criação de novas equipas com essa finalidade – integradas na Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática (CSIRT – *National Network of Computer Security Information Response Teams*). Por último, prevêem-se diversos mecanismos de reporte de incidentes ao Centro Nacional de Cibersegurança por parte de entidades e organismos públicos, de operadores de infraestruturas críticas e de serviços essenciais, bem como prestadores de serviços digitais.

52. Para uma revisão das estratégias e programas públicos no domínio da cibersegurança em Portugal, consultar o Relatório Cibersegurança em Portugal: Políticas Públicas 2021, do CNCS (Disponível em: https://www.cncs.gov.pt/docs/relatorio-politicaspublicas2021-observatoriociberseguranca-cncs-.pdf)

53. A Lei Orgânica do Gabinete Nacional de Segurança, estabelecida pelo Decreto-Lei n.º 3/2012, de 16 de janeiro, é alterada pelos Decretos-Lei n.º 162/2013, de 4 de dezembro, n.º 69/2014, de 9 de maio, e n.º 136/2017, de 6 de novembro.

54. Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril.

Em 2018, foi aprovado o Regime Jurídico da Segurança no Ciberespaço, através da Lei n.º 46/2018, de 13 de agosto, que transpõe a Diretiva (UE) n.º 1148/2016 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, sobre medidas para garantir um elevado nível comum de segurança das redes e de informação em geral e em toda a União Europeia. A Lei portuguesa prevê:

- A definição de uma nova Estratégia Nacional de Segurança do Ciberespaço, adaptada às necessidades impostas pela evolução das ameaças cibernéticas e dos riscos correspondentes;
- A identificação de um ponto de contacto único e da Autoridade Nacional de Cibersegurança – o Centro Nacional de Cibersegurança;
- Os protocolos de segurança TIC e dos requisitos e medidas de segurança das redes e sistemas de informação; e,
- As obrigações e procedimentos de notificação de incidentes, assim como o regime sancionatório.

O Regime Jurídico da Segurança do Ciberespaço é regulamentado através do Decreto-Lei n.º 65/2021. Este diploma estabelece: i) Os requisitos de segurança das redes e dos sistemas de informação que devem ser cumpridos pela Administração Pública, pelos operadores de infraestruturas críticas e pelos operadores de serviços essenciais; e, ii) Os requisitos de notificação de incidentes que afetem a segurança das redes e dos sistemas de informação que devem ser cumpridos pela Administração Pública, pelos operadores de infraestruturas críticas, pelos operadores de serviços essenciais e pelos prestadores de serviços digitais. Adicionalmente, este Decreto-Lei define as obrigações em matéria de certificação de cibersegurança.

Em 2019, foi publicada uma nova Estratégia Nacional de Segurança do Ciberespaço, para o período 2019-2023, que define o enquadramento, os objetivos e as linhas de ação do Estado em matéria de segurança do ciberespaço. Esta estratégia de âmbito nacional surge na sequência da transposição da referida Diretiva da Segurança das Redes e dos Sistemas de Informação. Tal como a estratégia de 2015, os princípios ou pilares deste documento estratégico são a subsidiariedade, a complementaridade, a cooperação, a proporcionalidade e a sensibilização. Os objetivos estratégicos definidos no âmbito desse documento são:

- Estruturar a segurança do ciberespaço;
- Prever, educar e sensibilizar em matéria de cibersegurança;
- Proteger o ciberespaço e as infraestruturas críticas;
- Melhorar a resposta às ameaças e combater o cibercrime;
- Apoiar a investigação, o desenvolvimento e a inovação; e,
- Fomentar a cooperação nacional e internacional.

Posteriormente, ainda em 2019, o Centro Nacional de Cibersegurança publicou o Quadro Nacional de Referência para a Cibersegurança (QNRCS), que é um guia de cibersegurança que elenca um conjunto de medidas para lidar com as principais problemáticas nesse domínio. O QNRCS constitui um referencial para que possam ser cumpridos os requisitos mínimos de segurança da informação recomendados.

Em matéria de resposta a incidentes existem duas iniciativas que merecem especial destaque. Em primeiro lugar, o CERT.PT que coordena a resposta a incidentes envolvendo entidades da Administração Pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais, bem como a totalidade do ciberespaço nacional. O CERT.PT é um serviço integrado no CNCS.

Em segundo lugar, a Rede Nacional de CSIRT (RNCSIRT) que é um fórum de partilha de informação de caráter operacional, constituída, atualmente, por mais de cinquenta entidades. Os principais objetivos desta rede são: i) promover um ambiente de cooperação e assistência recíproca entre os responsáveis pela segurança informática em matéria de tratamento de incidentes e partilha de boas práticas; ii) desenvolver indicadores e informação estatística sobre incidentes de segurança; iii) desenhar instrumentos de prevenção e resposta rápida perante incidentes de grande dimensão; e, iv) promover uma cultura de segurança no país. O CERT.PT é membro da RNCSIRT.

A criação desta arquitetura institucional e de um quadro normativo em matéria de cibersegurança tem posicionado Portugal entre os países do mundo mais avançados neste âmbito. De um ponto de visto económico, este contexto jurídico-institucional é fundamental para: i) reduzir a incerteza das empresas nacionais, ao produzir orientações em matéria de cibersegurança; ii) melhorar a regulação das empresas em geral e das entidades/infraestruturas críticas no domínio da cibersegurança; iii) alavancar o investimento no setor, tanto em investigação, desenvolvimento e inovação, como em desenvolvimento empresarial, especialmente através do apoio a *startups* na área da cibersegurança;[55] e, iv) atrair investimento direto estrangeiro ao país no setor das TIC e não só.

55. Neste âmbito é de destacar o trabalho realizado pelo Startup Portugal.

Em termos latos, a arquitetura institucional da cibersegurança em Portugal integra diferentes entidades:[56]

- O Gabinete Nacional de Segurança (GNS);
- O Centro Nacional de Cibersegurança (CNCS);
- A Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT), integrada no CNCS;
- O Conselho Superior de Segurança do Ciberespaço;
- A Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária (UNC3T);
- O Gabinete de Coordenação da Atividade do Ministério Público na Área da Cibercriminalidade;
- As Estruturas do Sistema de Informações da República Portuguesa (SIRP), ligadas à CIBERINTEL;
- O Comando para a Ciberdefesa do Estado Maior General das Forças Armadas (EMGFA); e,
- O Centro de Operações do Ciberespaço, vinculado à NATO.

Estas entidades trabalham em estreita colaboração com as suas congéneres Europeias. Por exemplo, o CNCS trabalha em articulação com a ENISA, o CERT.PT com a Rede Europeia de CSIRT[57] e a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária (UNC3T) com o Centro Europeu de Cibercriminalidade (EC3) da Europol.

2.4 OUTRAS INSTITUIÇÕES INTERNACIONAIS

Para além da União Europeia, em matéria de cibersegurança e cibercrime, Portugal tem beneficiado de outros referenciais e práticas, nomeadamente dos resultantes da atividade de diversas instituições internacionais. Em alguns casos, porque os instrumentos de *soft law* (Conselho da Europa) e as orientações, recomendações e boas práticas (Nações Unidas, OCDE) são muito valiosos para ancorar o desenvolvimento legislativo e a adoção de políticas públicas. Noutros casos, porque as iniciativas de capacitação (NATO), intercâmbio de informação (Nações Unidas, NATO) e cooperação internacional (Conselho da Europa, Nações Unidas, NATO) são fundamentais para gerir as ciberameaças, minimizar o impacto dos ciberataques e combater o cibercrime.

2.4.1 O CONSELHO DA EUROPA

O Conselho da Europa tem tido um papel de grande importância na sensibilização para os riscos dos ciberataques e do cibercrime. Em novembro de 2001, aprovou a Convenção de Budapest sobre Cibercrime, que tinha como finalidade última servir de orientação para que os países desenvolvam legislações nacionais integrais e harmonizadas para combater o cibercrime. Desta forma, os seus principais objetivos são harmonizar a legislação sobre cibercrime e melhorar a cooperação internacional. Trata-se, portanto, de estabelecer uma política criminal comum e alinhada entre países, que implica a tipificação dos crimes informáticos de forma similar em todos os Estados aderentes e uma cooperação internacional reforçada neste domínio.

Esta Convenção é o único instrumento internacional vinculante sobre cibercrime. Até 2021, a Convenção foi ratificada por 66 Estados, 45 membros do Conselho da Europa e 21 não-membros. Adicionalmente, 11 países têm estatuto de observadores e 158 países utilizaram a convenção como orientação nas suas legislações nacionais.

2.4.2 AS NAÇÕES UNIDAS

Para as Nações Unidas, a cibersegurança é uma dimensão de interesse crescente pelo seu caráter transversal. Entre as principais atividades desenvolvidas pela instituição neste âmbito destacam-se:

- O trabalho do Comité para o Desarmamento e a Segurança Internacional, que tem dedicado uma parte da sua atividade à discussão sobre as ameaças à segurança da informação. Este comité impulsionou a constituição de grupos de trabalho de peritos que estudam assuntos relacionados com as ameaças existentes e potenciais no ciberespaço, o comportamento responsável dos Estados-membros neste âmbito ou a aplicação do direito internacional;
- A atividade do Comité para as Questões Sociais, Humanitárias e Culturais e do Comité Económico e Financeiro, que têm adotado diversas resoluções relacionadas com a cibersegurança – cultura de cibersegurança, infraestruturas de informação, cibercrime e direito à privacidade, entre outras;
- O programa de Cibersegurança e Novas Tecnologias destinado a melhorar a capacidade dos Estados-membros e das organizações privadas para prever e mitigar a utilização de tecnologia por parte de terroristas e outros grupos violentos;
- A criação da figura de um Relator Especial sobre o direito à privacidade, com a finalidade de criar um contexto digital mais seguro;
- O aumento do interesse e da dedicação ao cibercrime do Conselho Económico e Social e do Congresso das Nações Unidas sobre Prevenção da Criminalidade e Justiça Criminal.

56. Para uma explicação aprofundada sobre os objetivos, funções e composição destas entidades, consultar o Relatório Ética e Direito 2020 do CNCS (Disponível em: https://www.cncs.gov.pt/docs/relatorio-eticadireito2020-observatoriocibersegurança-cncs.pdf).

57. O CERT.PT é membro da Rede Nacional de CSIRT e é o representante português na Rede Europeia de CSIRT.

Não obstante, as iniciativas das Nações Unidas com mais impacto operacional no âmbito da Cibersegurança são as desenvolvidas pela ITU, que é o organismo especializado da Instituição dedicado às Tecnologias de Informação e Telecomunicações. Uma das principais atividades da ITU é a promoção da confiança e a segurança na utilização das tecnologias de informação e comunicação.

Para dar cumprimento a esse desiderato, a ITU lançou em 2007 a *Agenda Global da Cibersegurança* (GCA), como quadro de referência para a cooperação internacional no âmbito da cibersegurança. Os principais projetos da ITU relacionados com a cibersegurança são: i) a conceção de estratégias de cibersegurança e a sua publicação; ii) a criação de equipas de resposta a incidentes informáticos (CSIRT); iii) o desenvolvimento de exercícios que contribuam para melhorar a preparação, proteção e as capacidades de resposta a incidentes; e, iv) a elaboração anual do *Índice Global Cibersegurança* (GCI), para medir o compromisso dos países com a mesma.

2.4.3 A ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO – OCDE

Outras instituições internacionais como a OCDE têm dado especial atenção à Cibersegurança, embora esta organização tenha preferência por utilizar o termo Segurança Digital. O trabalho da OCDE no domínio da segurança digital tem como finalidade desenvolver e promover políticas que reforcem a confiança sem limitar o potencial das TIC no apoio à inovação, à competitividade e ao crescimento. Como noutros âmbitos, a OCDE desenvolve diagnósticos exaustivos sobre a matéria e propõe aos países-membros a articulação de estratégias em torno do assunto em questão, neste caso a segurança digital.

O trabalho da OCDE sobre segurança digital é efetuado por um Grupo de Trabalho sobre Segurança na Economia Digital, que depende do Comité da OCDE sobre Políticas de Economia Digital. A finalidade última do Grupo de Trabalho é desenvolver e promover políticas baseadas na evidência que reforcem a segurança da economia digital.

A OCDE também disponibiliza *standards* internacionais na área de políticas de segurança digital. Neste âmbito tem efetuado recomendações sobre gestão de riscos na segurança digital para a prosperidade económica e social e sobre a segurança digital de atividades críticas. Também tem proposto orientações sobre políticas criptográficas.

A OCDE lançou, em 2018, o denominado Fórum Global sobre Segurança Digital para a Prosperidade. Trata-se de uma iniciativa de caráter internacional, multilateral e multidisciplinar que envolve comunidades de *stakeholders* desta área. Pretende servir de fórum para o intercâmbio de experiências e boas práticas em matéria de riscos da segurança digital e a sua gestão, para a aprendizagem conjunta e para a construção de convergências sobre segurança digital.

Os resultados do Fórum servem frequentemente para alimentar trabalhos com uma marcada componente de *policy,* que geralmente são incluídos na série de artigos da OCDE denominada OCDE *Digital Economy Papers.* Esta série cobre um amplo espectro de problemáticas das TIC e inclui estudos de diversa natureza para públicos muito variados.

Sendo a OCDE uma instituição dedicada ao estudo de temáticas económicas e à promoção de políticas públicas em diversos domínios económicos, a sua preocupação com as questões da cibersegurança é um reconhecimento da sua relevância em matéria económica e empresarial. Dada a reputação da OCDE, o rigor das suas análises e os fundamentos das suas sugestões de *policy*, as orientações e recomendações que propõe na área da cibersegurança têm um elevado valor acrescentado para a formulação de políticas a nível nacional e, inclusivamente, em âmbitos mais latos.

2.4.4 A ORGANIZAÇÃO PARA O TRATADO DO ATLÂNTICO NORTE – NATO

Dada a importância crescente que os ciberataques podem ter nos conflitos entre países e em situações de guerra, a NATO tem vindo a dar uma importância crescente à cibersegurança. Nos últimos anos, a NATO tem desenvolvido numerosos projetos na área do ciberespaço, nomeadamente nos domínios da partilha de informação e da cooperação e a formação para a ciberdefesa.

Em 2008, a NATO criou um Centro de Excelência de Defesa do Ciberespaço dedicado à investigação e à formação na área da Cibersegurança, localizado em Talin. Atualmente, as principais áreas de atuação do Centro são a tecnologia, as operações, a estratégia e o direito. Este centro organiza periodicamente exercícios de ciberdefesa. Em abril de 2021 celebrou-se o maior exercício deste tipo alguma vez realizado, denominado *Locked Shields,* com mais de 2.000 participantes. A NATO possui outros centros de formação na área das TIC e da ciberdefesa na Alemanha, Itália e Portugal.

Em 2012 foi criada, no âmbito da NATO, a Agência de Comunicações e Informações, com sede em Bruxelas e departamentos em Mons e na Haia. Destina-se a proteger as redes e infraestruturas de comunicação e informação da própria Aliança e dos seus membros. A Agência integra um Centro de Cibesegurança que dispõe de serviços especializados para antecipar, detetar, responder e recuperar de incidentes de cibersegurança. O centro também funciona como um *ciberhub* em tempo real para a partilha de informação, formação e conhecimento para os membros da NATO. A Agência lançou em 2019 a rede de Equipas de Resposta a Emergências Informáticas da Aliança.

Em 2017, a NATO, em conjunto com a União Europeia, criou o Centro de Excelência no Combate a Ameaças Híbridas (*Hybrid CoE*), com sede em Helsínquia. Trata-se de uma organização baseada numa rede de Estados dedicada a enfrentar ameaças híbridas de todos os tipos. Posteriormente, em 2018, para garantir uma maior coordenação operacional, fortalecer a cibersegurança e integrar o ciberespaço nas operações de defesa da NATO foi constituído um Centro de Operações do Ciberespaço, com sede em Bruxelas.

No âmbito da sua Política Integral de Ciberdefesa a NATO está comprometida com a utilização das suas capacidades para dissuadir, defender-se e responder a todo o tipo de ciberameaças. No quadro da sua Agenda 2030, a NATO impulsou uma nova política de cibersegurança, que pretende reforçar o ciberespaço como domínio de intervenção prioritário nos próximos anos.

Embora possa parecer que o trabalho da NATO no domínio da cibersegurança é pouco relevante do ponto de vista económico, existem duas dimensões em que tem uma importância indiscutível. Em primeiro lugar, a estabilidade: todos os desenvolvimentos da NATO na área da cibersegurança têm um contributo fundamental para a manutenção da paz e a mitigação de conflitos, que são aspetos fundamentais para a prosperidade dos países. Em segundo lugar, a investigação e desenvolvimento: muitos dos desenvolvimentos tecnológicos promovidos pela NATO para melhorar os níveis de cibersegurança dos seus aliados procedem de investigação fundamental de base militar, que, em alguns casos, alimenta posteriormente a investigação aplicada no âmbito civil, alavancando soluções na área da cibersegurança com impactos positivos em cidadãos, empresas e administrações.

DESTAQUES CAPÍTULO II

A arquitetura institucional e o quadro legal da cibersegurança em Portugal são muito influenciados pelos desenvolvimentos legislativos na União Europeia. O enquadramento jurídico-institucional da União é fundamental para reforçar a cibersegurança a nível macro, proteger infraestruturas e entidades críticas, reduzir a incerteza para a generalidade dos agentes económicos e dar segurança jurídica às empresas e aos cidadãos. Como complemento, recentemente, a Comissão Europeia tem lançado diversas iniciativas no domínio da cibersegurança que visam promover a inovação, potenciar o desenvolvimento de produtos e serviços europeus e aumentar a soberania estratégica, fomentar a criação e o crescimento de empresas no setor e aumentar a sua competitividade à escala global.

O ponto de partida para a elaboração do normativo da União sobre esta matéria é a Estratégia de Cibersegurança da União Europeia, publicada em 2013. A peça fundamental da arquitetura da cibersegurança na União é a Diretiva sobre a Segurança de Redes e Sistemas de Informação (Diretiva SRI), publicada em 2016. É relevante também o Regulamento relativo à Agência da União Europeia para a Cibersegurança (ENISA) e à certificação da cibersegurança das TIC, de 2019.

Estes diplomas obrigaram os Estados-membros a criar capacidades e instituições de cibersegurança, conceber e implementar estratégias nacionais neste âmbito e participar em mecanismos de cooperação e partilha de informação. Permitiram também desenvolver e potenciar instrumentos europeus de suporte na área da cibersegurança e apoiar iniciativas de desenvolvimento setorial à escala da União.

Em finais de 2020, a Comissão Europeia aprovou um pacote de medidas, destinado a atualizar os principais instrumentos legislativos em vigor, para adaptar o quadro europeu de cibersegurança às mudanças nos mercados e às novas ameaças cibernéticas. As principais medidas incluídas no pacote são: i) a Estratégia de Cibersegurança da União Europeia para a Década Digital; ii) uma proposta de revisão da Diretiva de Segurança de Redes e Sistemas Informação (SRI 2.0), que substitua a de 2016; e, iii) uma proposta de Diretiva sobre Resiliência de Entidades Críticas, que substitua a Diretiva de Proteção de Infraestruturas Críticas (PIC), de 2008.

A Comissão tem vindo a densificar a arquitetura institucional (unidades, redes, centros), a arquitetura regulamentar (instrumentos legislativos, referenciais, *standards*) e a arquitetura operacional (PPP, incluindo organizações privadas, *toolboxes*, medidas, quadros de resposta) a nível comunitário. Tem promovido também o apoio financeiro a iniciativas e projetos relacionados com a cibersegurança, através do Quadro Financeiro Plurianual, de Programas como o *Horizonte Europa* ou o *Europa Digital* e, mais recentemente, dos fundos *Repair* e *Prepare* do pacote *Next Generation*.

Em Portugal, as políticas públicas e os instrumentos legislativos no domínio da cibersegurança estão alinhados com as orientações da União Europeia. O ponto de partida é a Estratégia Nacional de Segurança do Ciberespaço, de 2015, que segue as orientações gerais da Estratégia da União Europeia para a Cibersegurança, e que foi posteriormente revista em 2019. O principal diploma legal em matéria de cibersegurança em Portugal é o Regime Jurídico da Segurança no Ciberespaço, que transpõe a Diretiva sobre a Segurança de Redes e Sistemas de Informação (Diretiva SRI). Do ponto de vista institucional, o elemento basilar é o Centro Nacional de Cibersegurança, que é a autoridade nacional nesta matéria.

Graças a esta arquitetura institucional e ao quadro normativo vigente em matéria de cibersegurança, Portugal possui bons indicadores em várias dimensões neste âmbito. De um ponto de vista económico, este contexto jurídico-institucional é fundamental para: i) reduzir a incerteza das empresas nacionais em aspetos relacionados com a cibersegurança; ii) melhorar a regulação das empresas em geral e das entidades/infraestruturas críticas neste domínio; iii) alavancar o investimento no setor; e, iv) atrair investimento direto estrangeiro ao país.

Para além das orientações da União Europeia, a construção do quadro institucional e jurídico da cibersegurança em Portugal tem beneficiado de outros referenciais e orientações, especialmente dos produzidos no âmbito de diversas instituições internacionais. Em alguns casos, os instrumentos de *soft law* (Conselho da Europa) e as orientações, recomendações e boas práticas (Nações Unidas, OCDE) são muito valiosos para ancorar o desenvolvimento legislativo e a adoção de políticas públicas – no domínio económico, por exemplo, em matéria de cibercriminalidade económica ou gestão de riscos e segurança digital. Noutros casos, as iniciativas de capacitação (NATO), intercâmbio de informação (Nações Unidas, NATO) e cooperação internacional (Conselho da Europa, Nações Unidas, NATO) são fundamentais para gerir as ciberameaças e minimizar o impacto dos ciberataques. Do ponto de vista económico, estas iniciativas contribuem para promover a confiança, manter a paz e mitigar conflitos e alavancar a investigação, o desenvolvimento e a inovação em cibersegurança.

CAPÍTULO III
PANORAMA DA CIBERSEGURANÇA NAS EMPRESAS
EUROPA E PORTUGAL

CAPÍTULO III
PANORAMA DA CIBERSEGURANÇA NAS EMPRESAS – EUROPA E PORTUGAL

3.1 ENQUADRAMENTO

Nos últimos anos, os processos de organização e gestão empresarial experimentaram mudanças muito significativas, em quase todos os casos, associadas a desenvolvimentos nas TIC. As mais notórias relacionam-se com a adoção de ferramentas para aumentar a presença digital das empresas e o seu posicionamento e, simultaneamente, para comercializar os seus produtos e serviços através de canais eletrónicos. Outras não menos importantes estão associadas à adoção de novos processos de administração, gestão e relacionamento com terceiros. A gestão dos dados recolhidos nessas interações, o *Big Data*, é cada vez mais utilizada pelas empresas para gerar valor. Por último, outras mudanças derivam da aceleração da digitalização em diferentes áreas funcionais, onde as tecnologias de identificação por rádio frequência, a robotização, a utilização da IA ou a interconexão de sistemas e dispositivos através da IoT têm vindo a ganhar espaço na operação das empresas em múltiplos setores de atividade.

O objetivo deste capítulo é duplo. Primeiramente, pretende-se apresentar o panorama atual e, sempre que possível, a evolução recente, das principais mudanças na atividade empresarial, derivadas da crescente interconexão eletrónica e da intensificação dos processos de digitalização, que tendem a elevar os riscos cibernéticos. Pretende-se também analisar as práticas de segurança das TIC adotadas pelas empresas para mitigar esses ciber-riscos. A abordagem assumida nesta componente do relatório é comparada, com a finalidade de mostrar o posicionamento das empresas portuguesas face à média da União Europeia e à situação nos restantes países da União.

A finalidade última do capítulo é aferir a situação do tecido produtivo português nos domínios da vinculação eletrónica de processos e funções, da digitalização e da segurança das TIC. Os dados utilizados procedem do Eurostat. A secção 3.1 dedica-se a analisar as alavancas que impulsionam o reforço da segurança das TIC, nomeadamente os avanços em termos de vinculação externa entre empresas e sistemas e a automatização de processos funcionalmente diversificados. A secção 3.2 apresenta as práticas, medidas e políticas de segurança das TIC nas empresas, assim como o nível de exposição a incidentes de segurança e as formas de minimizar os seus potenciais impactos.

3.2. AS ALAVANCAS

Nas últimas duas décadas as empresas foram incorporando dimensões digitais aos seus processos de produção, comercialização, distribuição e logística e administração, em geral. Embora, num primeiro momento, um número relativamente reduzido de empresas digitalizou algumas das suas atividades (nomeadamente as mais fáceis de digitalizar), em fases posteriores o fenómeno foi-se estendendo até que um número significativo e crescente de empresas nascem completamente digitalizadas, nomeadamente em alguns sectores de comércio e serviços.

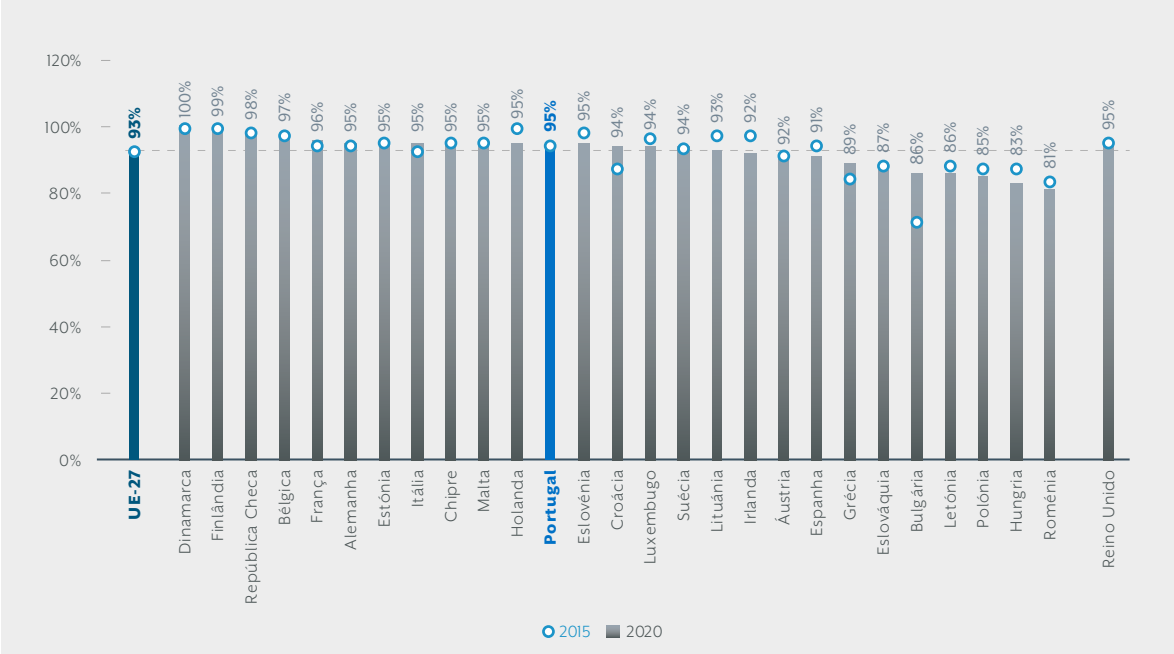
O crescimento da componente digital das empresas viu-se muito favorecido pela melhoria das infraestruturas digitais e pelo aumento da capacidade e velocidade das ligações à Internet. Os processos de digitalização empresarial, entendidos em sentido lato, aceleraram-se consideravelmente quando a melhoria da ligação à Internet permitiu às empresas operar em tempo real de forma rápida, confiável e segura.

Na Figura 3.1 apresenta-se a proporção de empresas com conexões DSL ou de banda larga fixa na União Europeia.[58] A cobertura de conexões de boa qualidade é em geral muito elevada. Em 2020, 93% das empresas europeias (UE-27) possuíam uma ligação à Internet de alta qualidade. Treze países apresentam percentagens iguais ou superiores a 95%, incluído Portugal, que neste indicador situa-se ligeiramente acima da média da União. Face aos dados de 2015, quer Portugal, quer a União Europeia, viram a sua posição melhorada num ponto percentual. Embora em alguns casos tenha havido retrocessos, na maioria dos países a cobertura das conexões à Internet de alta qualidade melhorou consideravelmente, nomeadamente entre aqueles mais atrasados em 2015.

As melhorias da ligação à Internet, a expansão do trabalho via plataformas e sistemas *cloud* e a interação permanente através do correio eletrónico e de outros sistemas de comunicação têm alavancado o crescimento do número de trabalhadores que usam computadores com ligação à Internet. Na Figura 3.2 consta a proporção de empregados que utilizam um computador ligado à rede no total do emprego nos países da União Europeia, em 2020 e 2015.

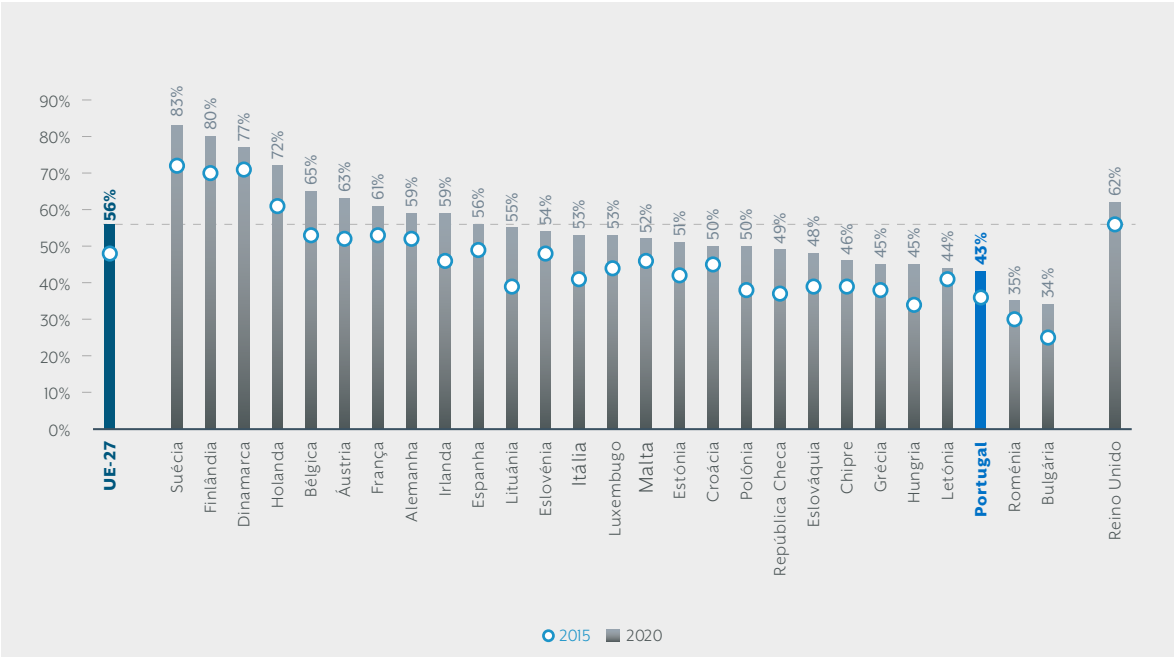
58. Nos gráficos desta secção, os dados dizem respeito ao ano mais recente para o que existem dados. Em alguns casos existem dados para 2020, mas noutros o último ano para o que existem dados é 2017. Sempre que existam dados para períodos prévios são efetuadas as correspondentes comparações – se possível em intervalos de cinco anos. Em bastantes casos, apenas existem dados para um ano, normalmente para 2019 ou 2020, pelo que não é possível efetuar essas comparações.

Figura 3.1 – Empresas que usam DSL ou outra conexão fixa de banda larga, 2020 | 2015, países da UE-27, % de empresas



Fonte: Eurostat.

Figura 3.2 – Empregados que usam computadores com ligação à Internet, 2020 | 2015, países da UE-27, % do emprego total

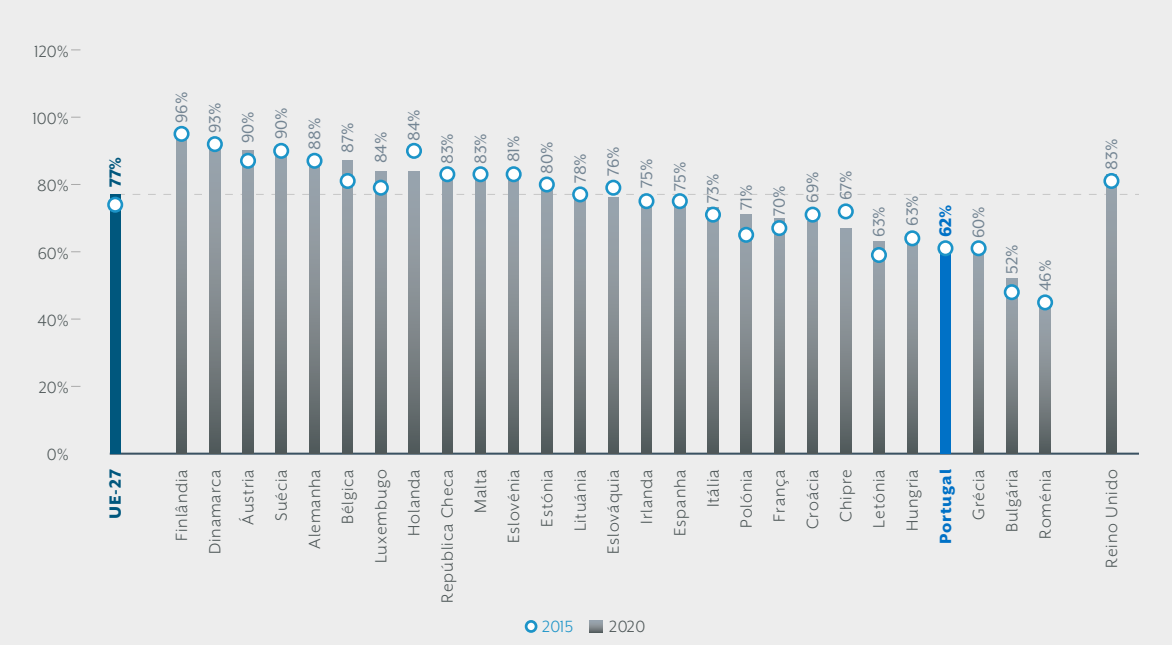


Nota: O dado para a Letónia na série de 2015 é de 2016 | Fonte: Eurostat.

Em 2020, 56% dos empregados no conjunto da União Europeia utilizava um computador com ligação à Internet. Nos países nórdicos essa percentagem situa-se à volta de 80% e noutros países da União, nomeadamente na Áustria, França e no Benelux acima dos 60%. Em Portugal, apenas 43% dos trabalhadores utilizam um computador ligado à Internet, treze pontos percentuais abaixo da média da UE, e apenas à frente dos dois países mais pobres do conjunto, a Bulgária e a Roménia. Entre 2015 e 2020, a percentagem de trabalhadores nestas circunstâncias avançou sete pontos percentuais face aos oito pontos da média da União – ou seja, em ambos os casos um crescimento similar, pouco superior a 16%.

A importância que as empresas atribuem à sua presença digital é dada pelo elevado número de empresas que dispõem de uma página de Internet ou de páginas nas redes sociais. A Figura 3.3 mostra a percentagem de empresas europeias que possuem um *site* na Internet.

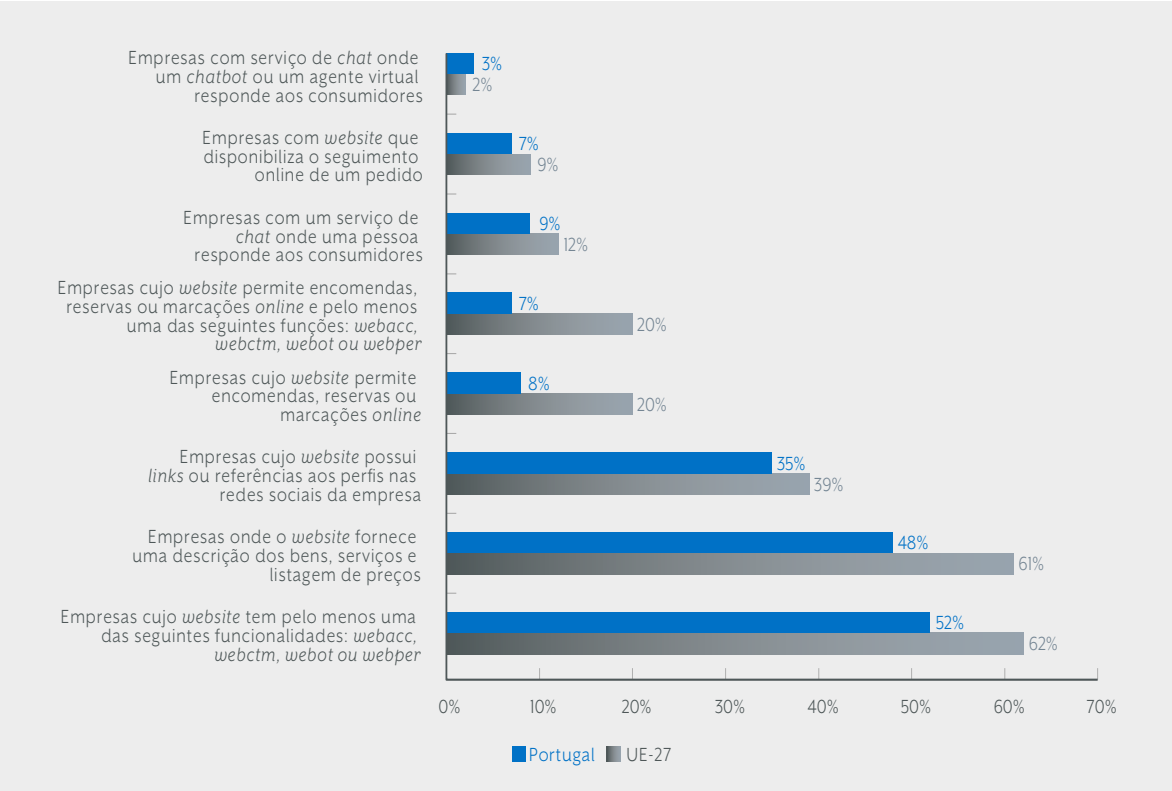
Figura 3.3 – Empresas com uma página de Internet, 2020 | 2015, países da UE-27, % de empresas



Fonte: Eurostat.

Em 2020, 77% das empresas europeias (UE-27) possuíam uma página de Internet, três pontos percentuais mais que em 2015. Em doze países, quatro em cada cinco empresas (ou mais) dispunham de uma página na Internet. Os países nórdicos e os do Norte da Europa são os que apresentam melhor desempenho neste indicador.

Figura 3.4 – Funcionalidades das páginas de Internet, 2020, Portugal | UE-27, % de empresas



Fonte: Eurostat.

Em Portugal, em 2020 só 62% das empresas possuíam um *site*, quinze pontos percentuais menos que a média da União Europeia. A melhoria nos últimos anos em Portugal foi marginal, de apenas um ponto percentual. Neste indicador Portugal unicamente está numa posição mais favorável que a Grécia, a Bulgária e a Roménia.

Em Portugal, em 2020 só 62% das empresas possuíam um *site*, quinze pontos percentuais menos que a média da União Europeia. A melhoria nos últimos anos em Portugal foi marginal, de apenas um ponto percentual. Neste indicador Portugal unicamente está numa posição mais favorável que a Grécia, a Bulgária e a Roménia.

Genericamente, as páginas de Internet das empresas portuguesas têm as mesmas funcionalidades das das empresas europeias, no entanto existem grandes diferenças em termos de intensidade de uso. Na Figura 3.4 constam as principais funcionalidades dos *sites* das empresas europeias e portuguesas, em 2020.

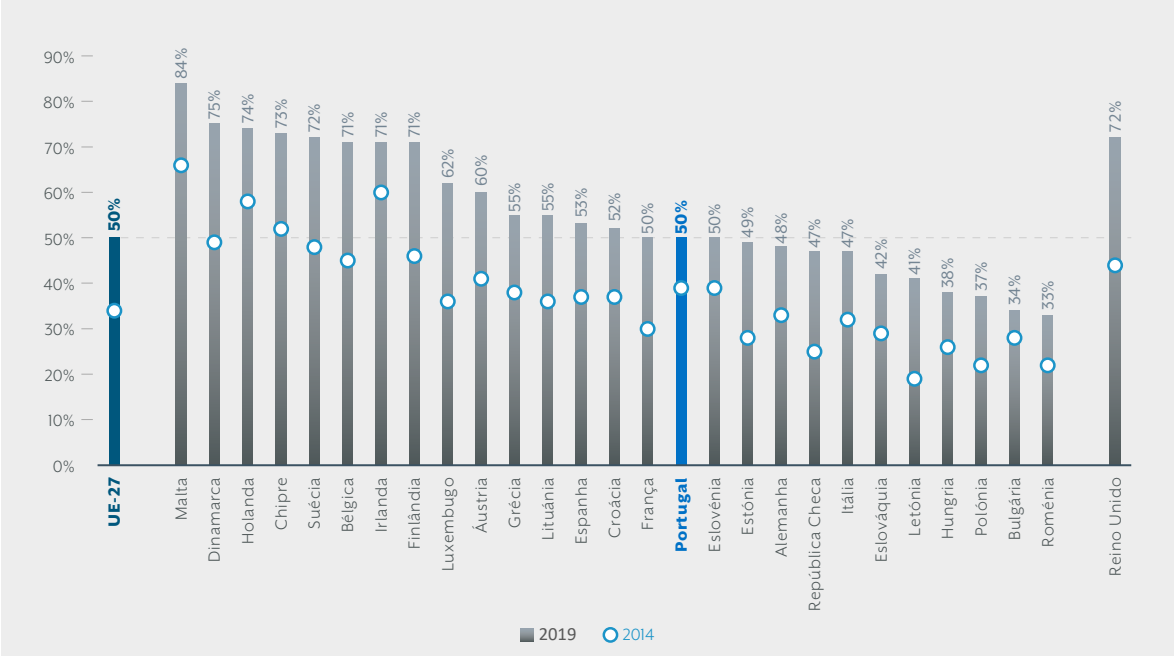
Excetuando numa das funcionalidades, em geral, os *sites* das empresas portuguesas dispõem de menos funcionalidades. Apenas no caso dos *sites* com um serviço de *chatbot* ou de um agente virtual que responde aos clientes, a proporção de empresas portuguesas que disponibilizam esta funcionalidade é superior à das empresas europeias (UE-27). Curiosamente, trata-se da funcionalidade menos frequente. Só 3% das páginas portuguesas e apenas 2% das europeias (UE-27) a disponibilizam.

A funcionalidade onde as empresas portuguesas estão mais atrasadas, em relação às suas congéneres europeias, é a de ordenamento, reservas e marcações *online* (e alguma outra funcionalidade). Contrariamente, onde existe mais proximidade em termos de oferta de funcionalidades é na disponibilização de ligações ou referências aos perfis nas redes sociais da empresa.

A presença digital das empresas também pode ser mensurada através da disponibilidade de redes sociais e de atividades associadas. Para além de tornar a empresa mais visível e servir de instrumento de comunicação das suas atividades, estas plataformas são um potente meio de interação com clientes, consumidores e outros *stakeholders* das organizações empresariais.

Na Figura 3.5 consta a percentagem de empresas europeias que possuem, pelo menos, uma rede social. Em 2019, 50% das empresas europeias (UE-27) possuía, pelo menos, uma rede social. Desde 2014, verifica-se um forte crescimento deste indicador, que aumentou dezasseis pontos percentuais, desde os 34%. Em oito países, sete em cada dez empresas (ou mais) têm, pelo menos, uma rede social. Tal como no caso das páginas de Internet, os países nórdicos e os do Norte da Europa são os que possuem empresas mais ativas neste domínio. A novidade neste âmbito é que as empresas dos países insulares da União Europeia, Malta, Chipre e Irlanda, também apresentam um excelente desempenho.

Figura 3.5 - Empresas com, pelo menos, uma Rede Social, 2019|2014, países da UE-27, % de empresas

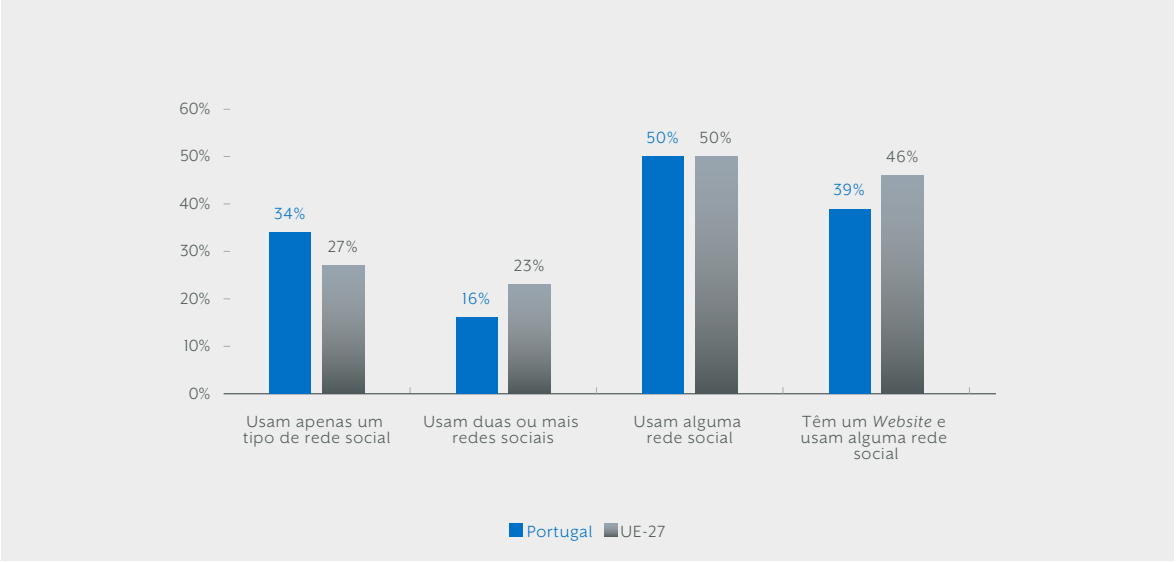


Fonte: Eurostat.

Neste caso Portugal situa-se na média da União Europeia, embora o progresso nos últimos cinco anos tenha sido inferior ao da média (onze pontos percentuais face aos dezasseis da média comunitária). No último quinquénio, todos os países da UE experimentaram progressos assinaláveis, especialmente os mais atrasados; não obstante, a proporção de empresas que dispõe deste tipo de presença digital continua a ser bastante inferior à das empresas que possuem páginas de Internet. O intenso crescimento no último quinquénio revela a importância que as empresas europeias atribuem a estes instrumentos de comunicação e interação.

A Figura 3.6 caracteriza a configuração da presença digital das empresas na União Europeia e em Portugal. Em ambos os casos, a maioria das empresas que possui uma página de Internet também tem presença nas redes sociais (46% na UE-27 e 39% em Portugal). No entanto, 27% das empresas europeias (UE-27) e 34% das empresas portuguesas apenas usam um tipo de rede social e não têm página de Internet. Isto revela que, para muitas empresas, as redes sociais são substitutas da página de Internet e que, provavelmente, lhes permitem dispor de funcionalidades adicionais. A relevância das redes sociais manifesta-se ainda no facto de que quase uma em cada quatro empresas europeias (UE-27) e mais de seis em cada dez empresas portuguesas usam duas ou mais redes sociais para aumentar o alcance da sua presença digital.

Figura 3.6 – Redes sociais e páginas de Internet, 2019, UE-27 | Portugal, % de empresas

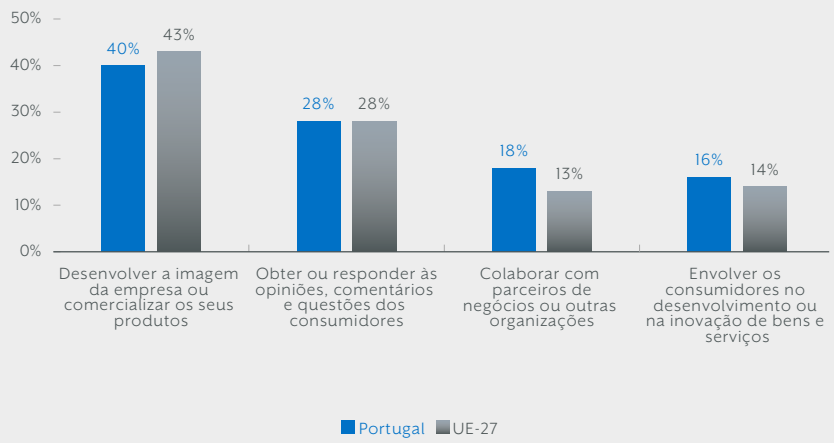


Fonte: Eurostat.

Genericamente, o uso das redes sociais está muito orientado para as questões da imagem, a comercialização e a interação com os clientes atuais e potenciais. Na Figura 3.7 pode constatar-se que as empresas portuguesas usam as redes sociais para os mesmos fins e com uma intensidade similar aos das empresas europeias. Em 43% das empresas europeias (UE-27) e em 40% das portuguesas as redes sociais são empregues para desenvolver a sua imagem e comercializar os seus produtos e serviços. Quase três em cada dez empresas (28%), tanto na Europa (UE-27) como em Portugal, utilizam as redes sociais para interagir com os seus clientes. Uma maior proporção de empresas portuguesas que de empresas europeias utilizam as redes sociais para colaborar com *stakeholders* (18% versus 13%) e promover o desenvolvimento e a inovação de produtos e serviços, especialmente com os consumidores (16% versus 14%).

Para além da sua presença digital, uma proporção considerável de empresas realiza vendas *online*. Muitas, inclusivamente, são nativas digitais e apenas vendem *online*. A percentagem de empresas que vendem através dos canais eletrónicos cresce anualmente a ritmos extremamente altos. A Figura 3.8 apresenta a percentagem de empresas europeias com vendas através de comércio eletrónico (via páginas de Internet, *apps* e *marketplaces*), em 2020 e 2015. Na União Europeia (UE-27), 21% das empresas realizam vendas *online*. Essa proporção quase duplica nos países líderes nesse indicador (Irlanda, 39%, e Dinamarca, 38%). Em doze dos vinte e sete países da UE, pelo menos uma em cada quatro empresas realizam vendas através de *e-commerce*. Tal como na média da União, em Portugal uma em cada cinco empresas realiza vendas eletrónicas (21% do total).

Figura 3.7 – Uso das redes sociais por propósito, 2019, UE-27 | Portugal, % de empresas



Fonte: Eurostat.

Nos últimos cinco anos, tanto no conjunto da União Europeia como em Portugal, a percentagem de empresas com vendas *online* aumentou marginalmente (21% versus 19%, na UE-27, e 21% versus 20%, em Portugal). Contrariamente, o incremento das vendas das empresas via *e-commerce* foi muito intenso na Áustria, Dinamarca, Roménia, Croácia, Lituânia e Espanha. Nestes últimos três países, o crescimento foi muito expressivo entre 2019 e 2020, devido aos efeitos da pandemia de Covid-19. Da mesma forma, em Portugal esse crescimento interanual foi também muito significativo, dado que, após vários anos de estagnação e uma quebra de três pontos percentuais em 2019, em 2020 a percentagem de empresas com vendas *online* cresceu quatro pontos percentuais.

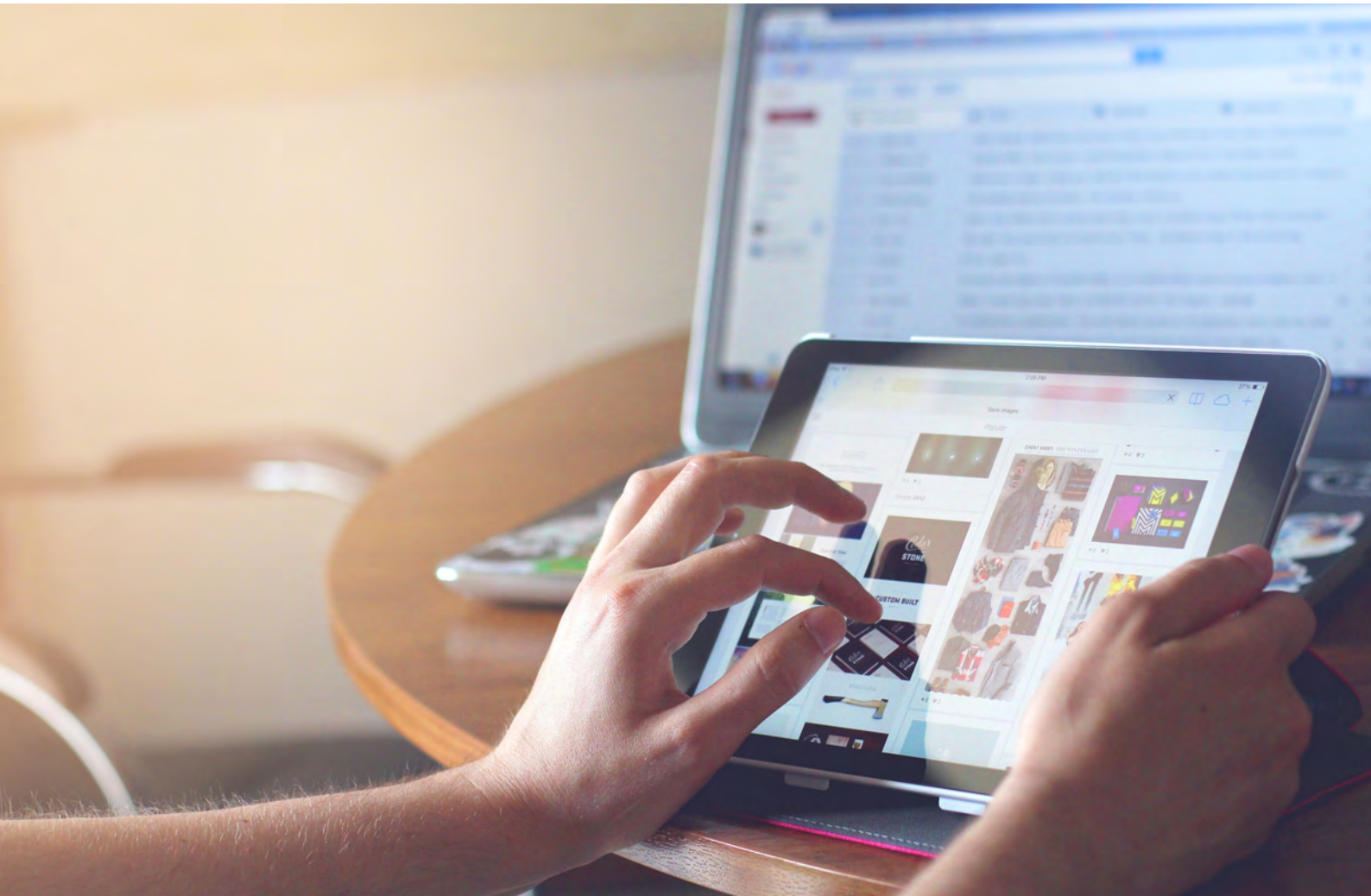
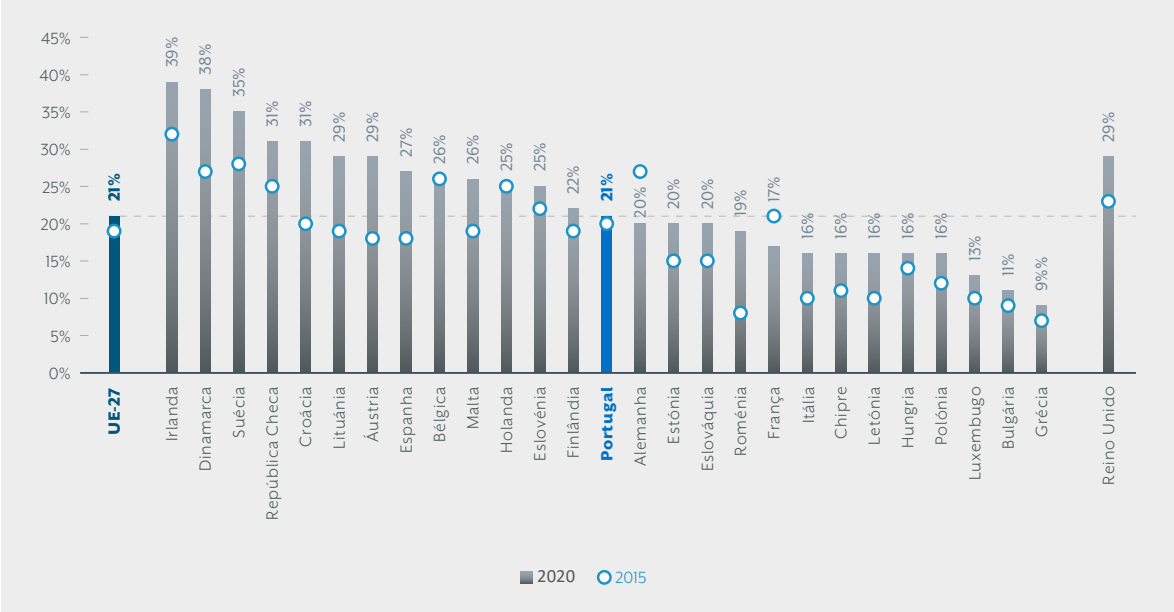


Figura 3.8 – Empresas com vendas através de comércio eletrónico, 2020 | 2015, países da UE-27, % de empresas



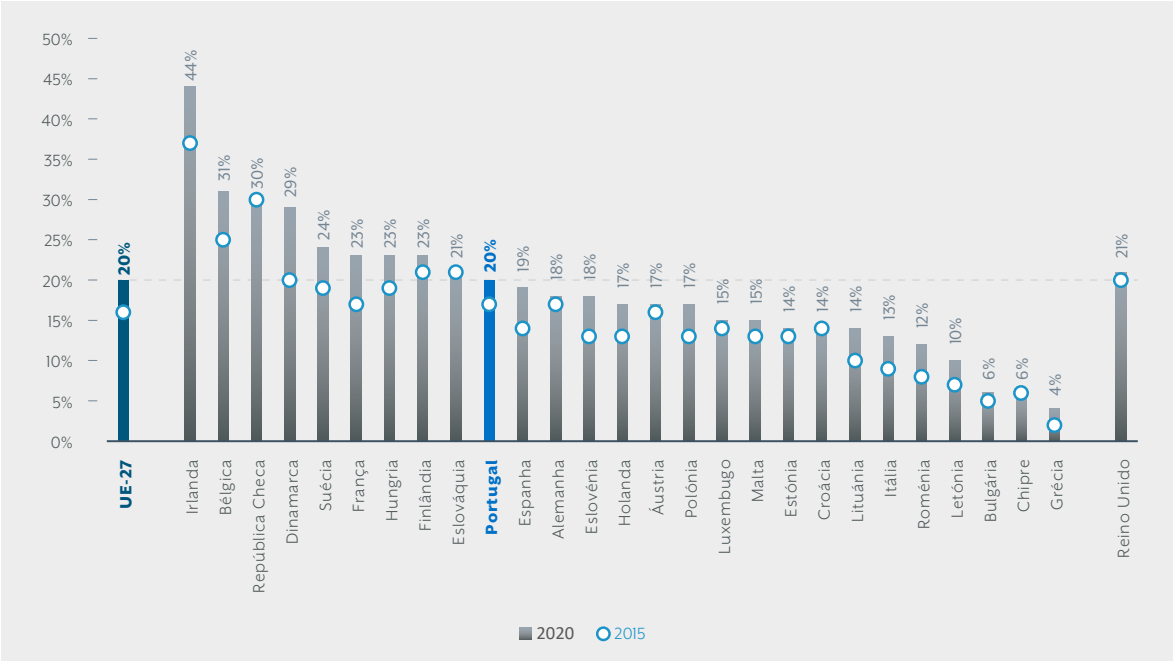
Nota: O dado da Grécia na série de 2020 é do ano 2019 | Fonte: Eurostat.

Relativamente às vendas B2B (*Business-to-Business*) e B2G (*Business-to-Government*), em 2020, 11% e 9% das empresas da UE-27 e de Portugal, respetivamente, realizaram vendas enquadráveis nestas modalidades. Em termos tendenciais, observa-se uma estagnação a nível da União Europeia e uma importante volatilidade em Portugal.

O crescimento relativo das empresas que vendem *online* tem impulsionado o crescimento do volume de negócios obtido por essa via. A Figura 3.9 mostra o peso da faturação das vendas eletrónicas no volume de negócios das empresas europeias, em 2020 e 2015. Tal como na Figura 3.8 observa-se um reforço das vendas *online*. Em 2020, 20% das receitas das empresas europeias (UE-27) procediam do negócio *online*, enquanto que em 2015 eram apenas 16%. Na Irlanda o peso das vendas via *e-commerce* alcança os 44%. Dos restantes países, nos três com melhor desempenho as vendas *online* representam à volta de 30% do volume de negócios das empresas.

Em Portugal, tal como para a média da UE-27, um em cada cinco euros de volume de negócios das empresas procede das vendas eletrónicas. Isto supõe um reforço de três pontos percentuais face a 2015 (17%, em 2015, *versus* 20%, em 2020). A análise conjunta destes dados e dos que são apresentados na Figura 3.8 permite concluir que o volume de faturação por empresa procedente das vendas *online* em Portugal aumentou entre 2015 e 2020.

Figura 3.9 – Volume de negócios das empresas procedente de vendas através de comércio eletrónico, 2020 | 2015, países da UE-27, % de empresas



Notas: O dado da Finlândia na série de 2020 é do ano 2019; os dados da Letónia e de Malta na série de 2015 são do ano 2016, e o do Luxemburgo do ano 2017. | Fonte: Eurostat.

O crescimento do comércio eletrónico na Europa em 2020 atingiu os 10%.[59] O setor representa 4,3% do PIB europeu e um valor agregado de 757.000 milhões de euros.[60] Em 2020, o comércio eletrónico cresceu menos que em 2019, quando o volume de negócios apresentou uma variação positiva de 14%. A desaceleração do ritmo de crescimento em 2020, motivado pela pandemia, justifica-se pelo impacto da crise sobre os sectores líderes em *e-commerce*: o turismo e o lazer.

Não obstante, a perda de atividade nesses sectores foi parcialmente compensada pelo crescimento do negócio *online* dos *retailers* da indústria da moda. Os sectores que mais cresceram em 2020 foram a moda, os conteúdos *streaming*, a decoração e o mobiliário e o *delivery* de restauração e alimentação.

Em Portugal, em 2021, 40,4% da população[61] efetuou compras *online*, face a 35,2% em 2020.[62,63] Não obstante, observa-se uma diminuição do número de encomendas realizadas e dos montantes despendidos. A maioria dos utilizadores de comércio eletrónico em Portugal encomendou produtos físicos (98,7%), enquanto aproximadamente metade declaram ter encomendado serviços (52,9%) e produtos em formato digital (50,3%). Entre as tipologias de produtos físicos encomendados pelos consumidores portugueses, em 2021, destacam-se a roupa, o calçado e os acessórios de moda (69,0%), as refeições em *takeaway* ou com entrega ao domicílio (46,0%). Entre os produtos digitais predominam os filmes, as séries ou os programas de desporto (34,9%) e entre os serviços, as reservas de alojamento *online* (28,0%.), os transportes (22,5%.) e as ligações à Internet, telefone e telemóvel (19,1%).

Para além das vendas *online*, existe um número muito significativo e crescente de empresas que realizam compras *online*. Na Figura 3.10 apresenta-se a percentagem de empresas europeias (UE-27) que efetuaram compras eletrónicas, em 2018 e 2013.

Em 2018, 44% das empresas europeias (UE-27) efetuaram compras *online*, dez pontos percentuais mais do que em 2013. Quase 80% das empresas suecas realizam este tipo de compras. Os restantes países nórdicos, assim como Áustria, Holanda, República Checa, Alemanha, Irlanda e França apresentam percentagens superiores a 50%. Os países onde mais cresceu a percentagem de empresas que adquirem bens e serviços *online*, nos cinco anos do horizonte temporal de análise, foram Suécia, França, Bélgica, Letónia e Chipre. Em Portugal só 28% das empresas compra *online* (2018). Tal como no conjunto da UE, no quinquénio analisado essa percentagem aumentou dez pontos percentuais, o que, no caso português, representa um crescimento superior a 55%.

59. B2C

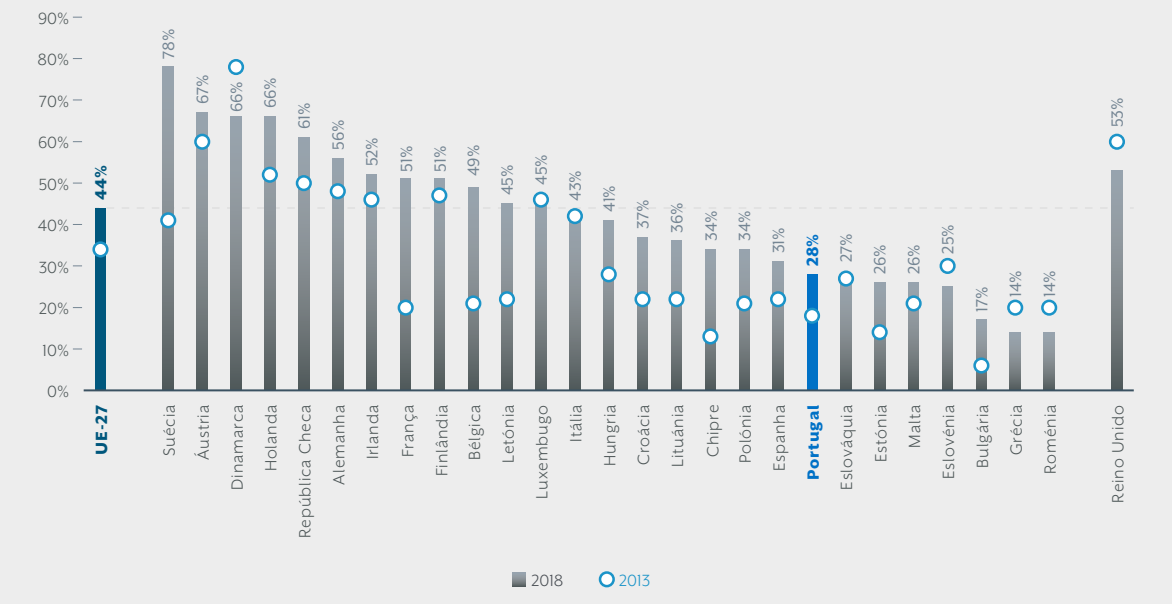
60. Ecommerce Europe (2021) (Disponível em: https://ecommerce-europe.eu/wp-content/uploads/2021/09/2021-European-E-commerce-Report-LIGHT-VERSION.pdf).

61. Na faixa dos 16 aos 74 anos.

62. Fizeram compras *online* nos últimos três meses.

63. INE (Destaque do INE – Inquérito à Utilização de Tecnologias da Informação e da Comunicação pelas Famílias 2021).

Figura 3.10 – Empresas que realizam compras *online*, 2018|2013, países da UE-27, % de empresas

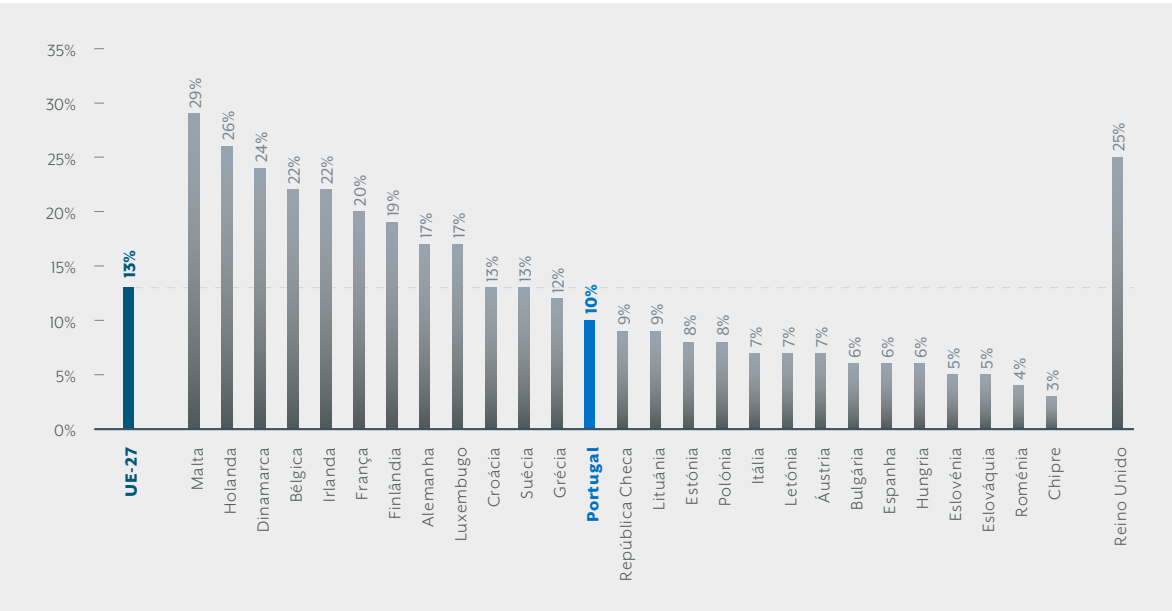


Notas: Na série de 2018, os dados da UE-27 e da Alemanha, França, Itália, Áustria e Eslovénia são do ano 2017. Os dados de Malta e Finlândia são do ano 2015. Dados mais recentes indisponíveis. | Fonte: Eurostat.

Os mecanismos de interação das empresas com o exterior (redes sociais, páginas de Internet, plataformas de vendas, compras, gestão de clientes, etc.) e outros instrumentos para melhorar processos e desempenhos produzem ingentes volumes de dados que são fontes de geração de valor potencial para as empresas. A análise e utilização de dados por parte das empresas têm vindo a acelerar-se nos últimos anos. A Figura 3.11 apresenta a percentagem de empresas europeias que analisam internamente o *Big Data* gerado a partir de qualquer fonte, em 2020. Em média, 13% das empresas europeias (UE-27) realizam esse tipo de análise. Em seis países, liderados por Malta, mais de 20% das empresas analisam internamente o seu *Big Data*. Portugal situa-se numa posição intermédia. Uma em cada dez empresas examina os dados produzidos no âmbito da sua atividade para fins de geração de valor.

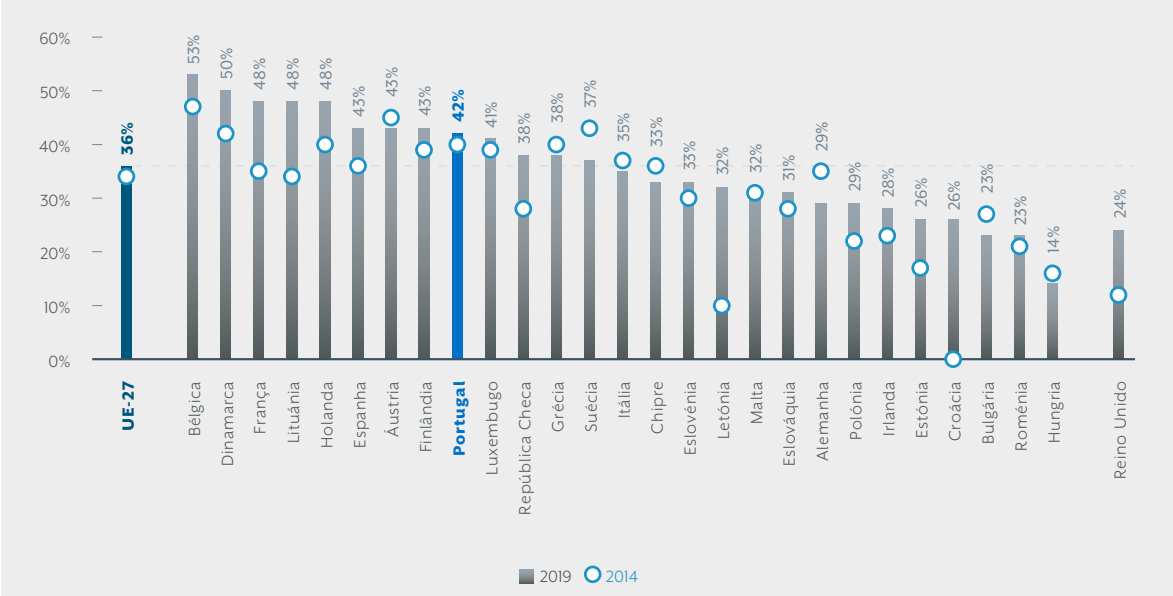
Para além das conexões cibernéticas com o exterior, as empresas estão a adotar crescentemente sistemas informáticos que permitem melhorar a integração entre diferentes áreas funcionais da empresa, e entre a empresa e os seus clientes. A Figura 3.12 mostra a percentagem de empresas europeias que utilizavam *software* ERP (*Enterprise Resource Planning* – Planeamento de Recursos Empresariais) para a partilha de informação entre diferentes áreas funcionais, em 2019 e 2014.

Figura 3.11 – Análise de *Big Data* internamente a partir de qualquer fonte, 2020, países da UE-27, % de empresas



Fonte: Eurostat.

Figura 3.12 – Empresas que possuem *software* de Planeamento de Recursos Empresariais – *Entreprise Resource Planning* (ERP) para a partilha de informação entre diferentes áreas funcionais, 2019|2014, países da UE-27, % de empresas

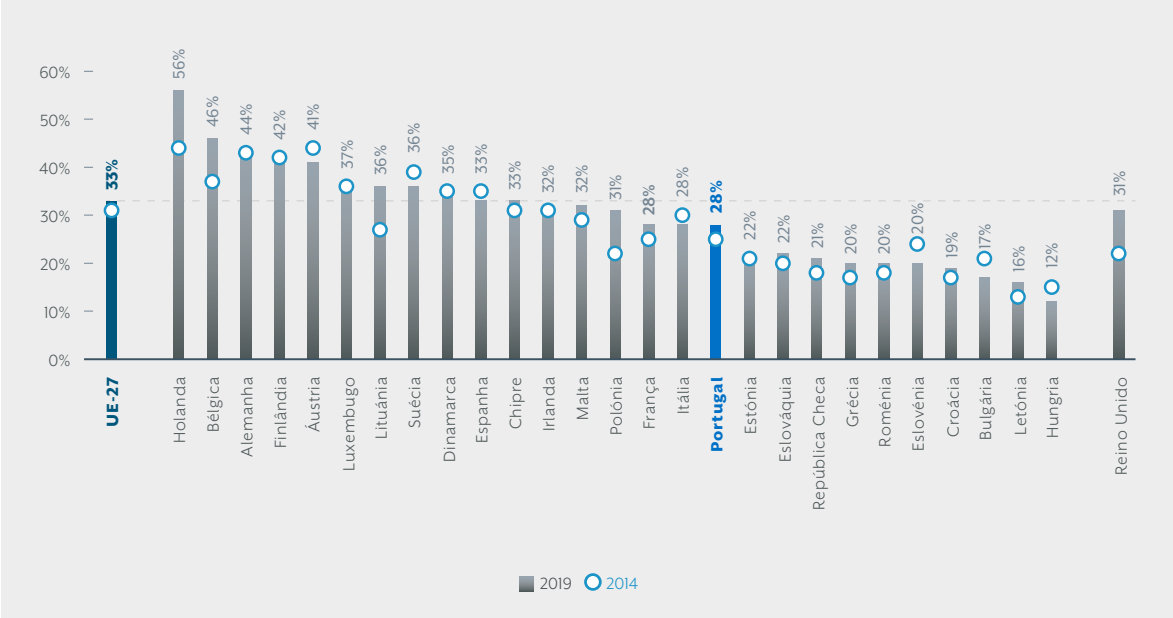


Fonte: Eurostat.

Na União Europeia (UE-27), 36% das empresas utilizam estes sistemas, existindo um avanço de dois pontos percentuais face à situação de 2014. Na Bélgica e na Dinamarca, uma em cada duas empresas utilizam sistemas ERP para a partilha de informação. Entre 2014 e 2019, França, Lituânia, República Checa e Letónia experimentaram avanços significativos neste indicador. Os sistemas ERP são utilizados por 42% das empresas portuguesas, tendo-se registado avanços pouco expressivos nos últimos cinco anos (apenas dois pontos percentuais).

No âmbito do seu relacionamento com clientes, as empresas recorrem a ferramentas informáticas que facilitam a gestão das interações. Na Figura 3.13 apresenta-se a percentagem de empresas europeias que utilizavam programas CRM (*Customer Relationship Management* – Gestão do Relacionamento com Clientes) para gerir a relação com os seus clientes, em 2019 e 2014. Uma em cada três empresas europeias (UE-27) utiliza este tipo de *software* com esse fim, uma proporção muito similar à de cinco anos antes.

Figura 3.13 – Empresas que utilizam *software* para gerir a relação com os seus clientes – *Costumer Relationship Management* (CRM), 2019|2014, países da UE-27, % de empresas

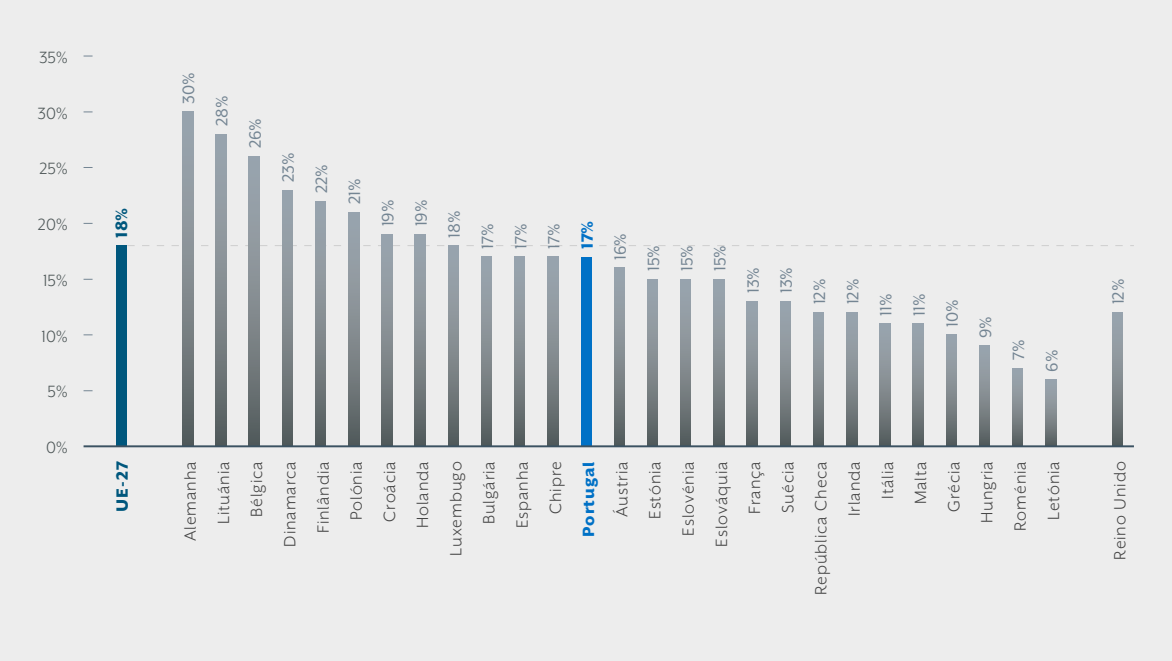


Fonte: Eurostat.

As empresas da Holanda, Bélgica e Alemanha são as que mais recorrem a estas ferramentas, enquanto que as da Bulgária, Letónia e Hungria são as que menos. Nos últimos anos, os países que mais avançaram na incorporação destes programas de gestão foram a Bélgica, a Lituânia e a Polónia. Em Portugal, quase três em cada dez empresas (28%) utilizam *software* CRM, embora os progressos dos últimos cinco anos tenham sido relativamente modestos (três pontos percentuais).

Além do seu relacionamento digital com clientes, as empresas também estabelecem vínculos similares com os seus fornecedores. Na Figura 3.14 pode visualizar-se a percentagem de empresas europeias com processos de negócio automaticamente vinculados aos dos seus fornecedores e clientes, em 2017. Em 18% das empresas europeias (UE-27) existem deste tipo de vínculos com os seus parceiros de negócio.

Figura 3.14 – Empresas cujos processos de negócio estão automaticamente vinculados aos dos seus fornecedores e/ou clientes, 2017, países da UE-27, % de empresas



Fonte: Eurostat.

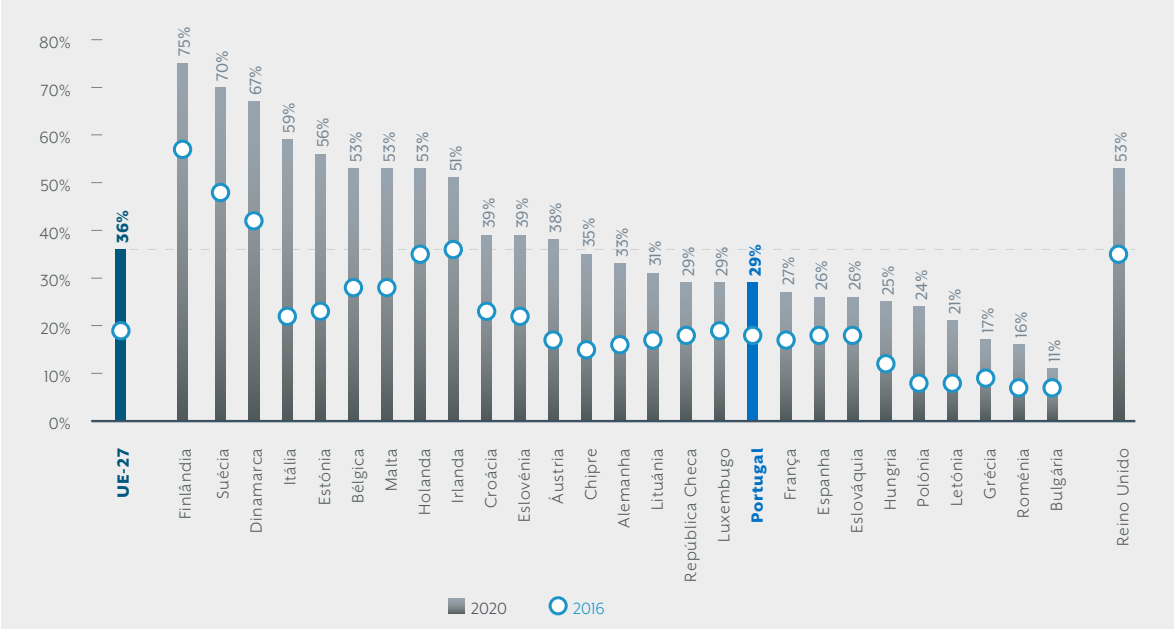
Os vínculos automáticos estão bastante generalizados na Alemanha (30% das empresas), na Lituânia (28%) e na Bélgica (26%), sendo uma prática pouco frequente entre as empresas da Hungria (95), da Roménia (7%) e da Letónia (6%). Em Portugal, 17% das empresas dispõem de mecanismos automáticos de vinculação com fornecedores e/ou clientes.

As empresas estão a adotar novos processos para reduzir custos e melhorar o desempenho e a eficiência dos equipamentos e das organizações no seu conjunto. Uma das políticas que tem vindo a ganhar preponderância a nível empresarial é o recurso a serviços na nuvem. A Figura 3.15 apresenta a percentagem de empresas europeias que adquiriram serviços *cloud*, em 2020.

Em 2020, 29% das empresas portuguesas adquiriu serviços *cloud*, face a 18% em 2016. A adoção crescente deste tipo de serviços, observada para a média da União, é transversal a todos os países da UE-27, embora os progressos em Espanha, Eslováquia e França, entre 2016 e 2020, tenham sido modestos em termos relativos.

Nesse ano, 36% das empresas europeias (UE-27) compraram serviços com alojamentos *cloud*. Neste campo tem havido uma progressão muito significativa, dado que em 2016 essa percentagem era da ordem dos 19%. Nos países nórdicos, mais de duas em cada três empresas recorrem a este tipo de serviços, enquanto na Grécia, na Roménia e na Bulgária menos de uma em cada cinco adota esta estratégia de contratação descentralizada.

Figura 3.15 – Compra de serviços de computação na nuvem (*cloud computing*), utilizados através de Internet, 2020, países da UE-27, % de empresas

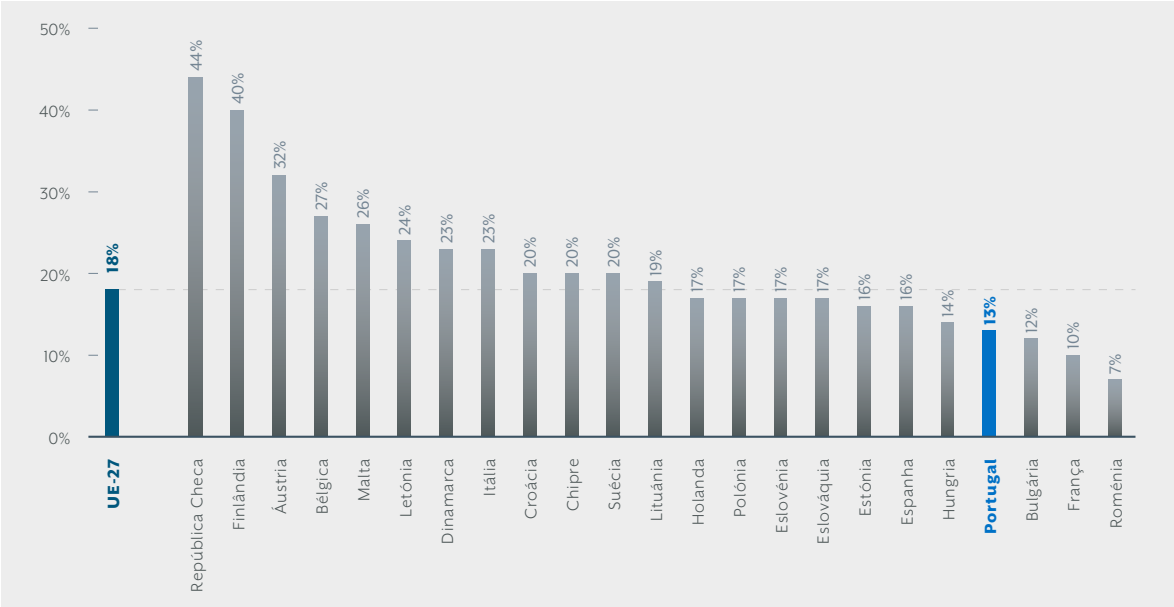


Fonte: Eurostat.

Uma outra das estratégias das empresas para melhorar o seu desempenho funcional e geral e elevar a eficiência dos seus sistemas e dispositivos consiste em potenciar a sua interconexão eletrónica através da Internet. A Figura 3.16 apresenta a percentagem de empresas que utilizam sistemas ou dispositivos suscetíveis de monitorização ou controlo remoto através da Internet. Em 2020, 18% das empresas europeias (UE-27) usava dispositivos ligados à IoT. As empresas da República Checa, da Finlândia e da Áustria são as que mais utilizam esta tecnologia de monitorização e controlo automático remoto, em termos relativos. As que menos a utilizam são as da Bulgária, da França e da Roménia.

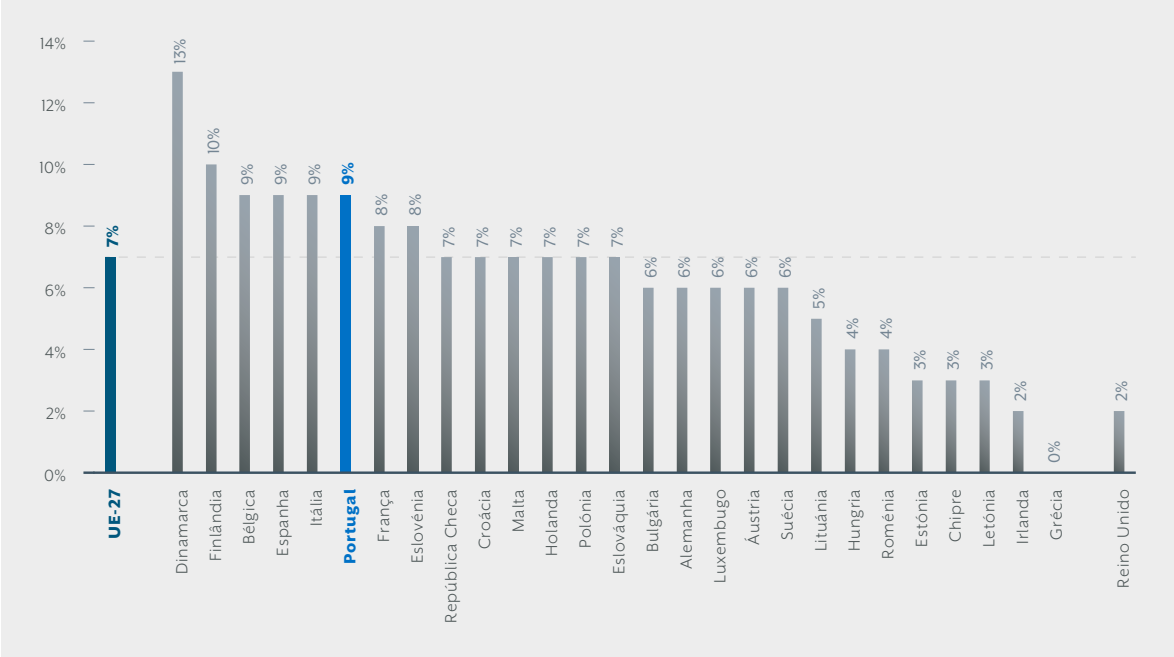
Portugal é o quarto país a contar da cauda do *ranking*, com apenas 13% das empresas a utilizarem sistemas e dispositivos ligados à IoT. Dada a falta de dados de exercícios anteriores não é possível analisar a evolução da adoção destas tecnologias, mas existem evidências ocasionais de que as empresas europeias, especialmente as industriais, estão a adotá-las de forma massiva.

Figura 3.16 – Uso de sistemas ou dispositivos interconectados, que podem ser monitorizados ou controlados remotamente através da Internet (IoT), 2020, países da UE-27, % de empresas



Notas: Não existem dados para Alemanha, Grécia, Irlanda e Luxemburgo. | Fonte: Eurostat.

Figura 3.17 – Uso de *robots* industriais ou de serviços, 2020, países da UE-27, % de empresas



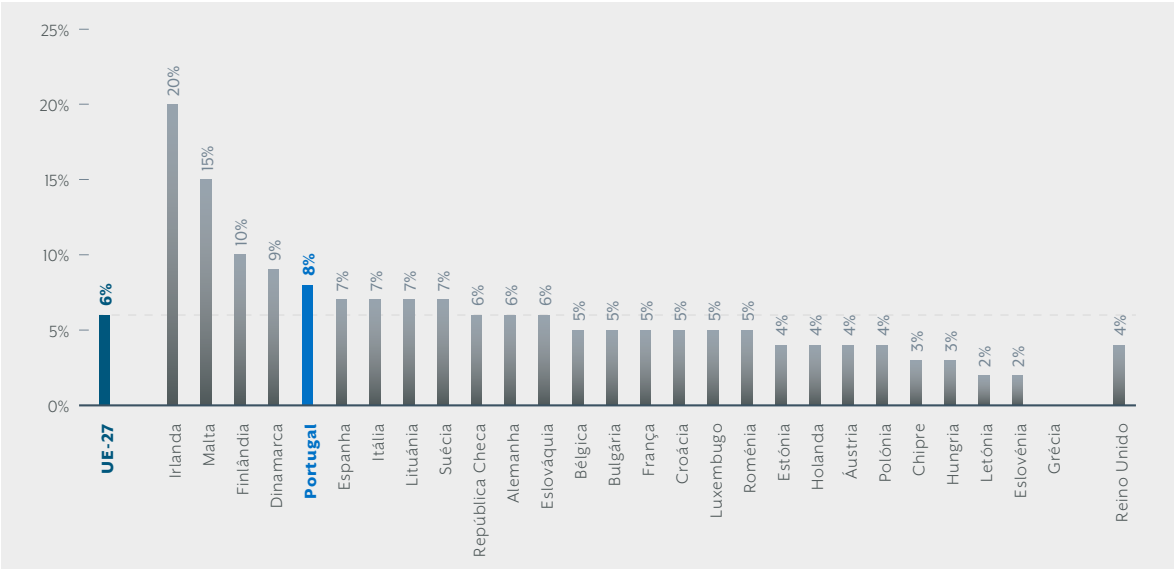
Notas: Não existem dados para Grécia. | Fonte: Eurostat.

Para além da presença digital e das vendas e compras *online*, da vinculação com clientes e fornecedores e entre sistemas e dispositivos existem outras dimensões que estão a acelerar e intensificar a digitalização das empresas europeias, nomeadamente a robotização e o recurso à IA. A Figura 3.17 mostra a percentagem de empresas europeias que usavam *robots* industriais e de serviços, em 2020.

Atualmente, 7% das empresas europeias (UE-27) utilizam *robots*, ainda que na Dinamarca e na Finlândia as percentagens sejam bastante mais elevadas (13% e 10%, respetivamente). Portugal situa-se imediatamente atrás desses dois países, dado que 9% das empresas portuguesas usam *robots* na sua atividade corrente, tal como na Bélgica, em Espanha e em Itália, que apresentam a mesma percentagem. A robotização em alguns países, especialmente naqueles com estruturas produtivas com escasso peso industrial, ainda está relativamente atrasada.

A IA é outra das tecnologias que está a ganhar terreno nas empresas no âmbito da digitalização empresarial. A Figura 3.18 apresenta a percentagem de empresas europeias que usam, pelo menos, um sistema de IA; 6% das empresas da União (EU-27) utilizavam, em 2020, um sistema deste tipo nas suas operações.

Figura 3.18 – Empresas que usam, pelo menos, um sistema de IA, 2020, países da UE-27, % de empresas



Notas: Não existem dados para Grécia. | Fonte: Eurostat.

Irlanda, Malta e Finlândia integram o top três neste indicador a nível da União Europeia (20%, 15% e 10% das empresas, respetivamente). Portugal emerge em quinto lugar. Em 8% das empresas portuguesas utiliza-se, pelo menos, um sistema de IA. Num número significativo de países, a adoção destes sistemas é ainda muito reduzida, dado que menos de 5% das empresas recorrem a estas tecnologias nos seus processos internos.

Em síntese, a maioria das empresas portuguesas tem vindo a aumentar a sua exposição digital, em consequência das melhorias de conectividade e das suas estratégias para potenciar a sua visibilidade e negócio digitais. Os indicadores de vendas *online* das empresas portuguesas são similares às das suas congéneres europeias, mas os de compras *online* são claramente inferiores.

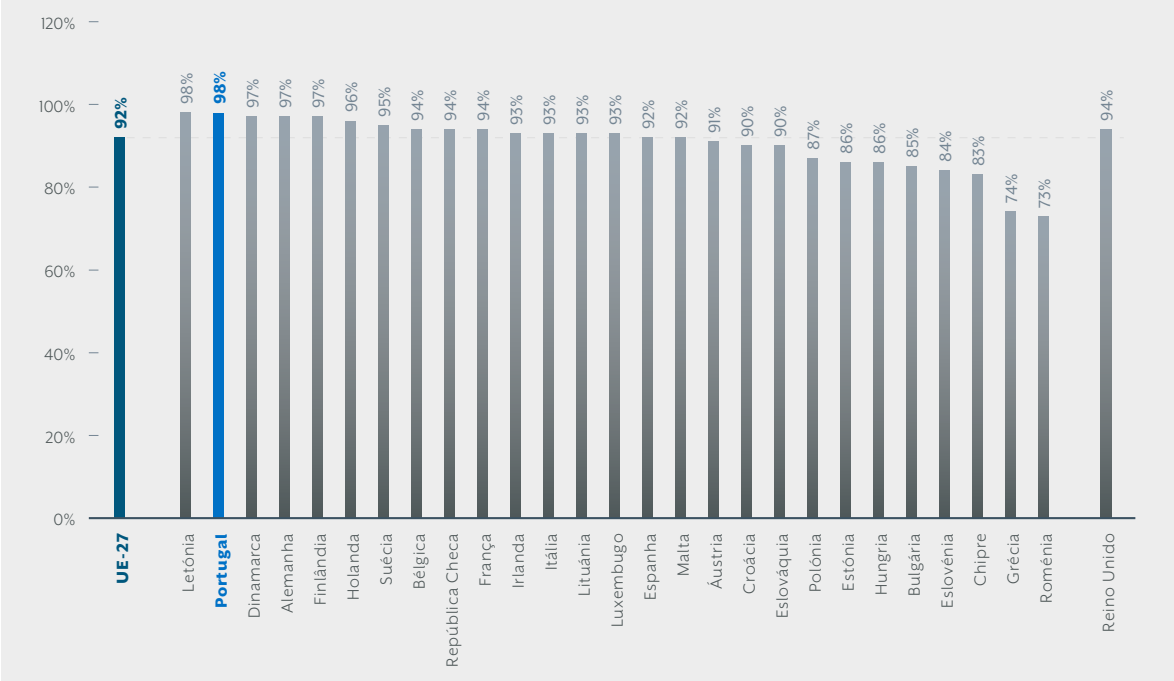
As empresas portuguesas também estão abaixo da média comunitária na incorporação de soluções *cloud*, no uso de *Big Data* e na adoção de sistemas ou dispositivos interconectados através da Internet (IoT). Embora atrasadas em relação à média, a situação altera-se no que se refere à adoção de sistemas de integração com clientes e fornecedores. Contrariamente, em relação a sistemas mais sofisticados de fabrico e interação automática, tais como os *robots* industriais e de serviços e os sistemas de IA, a adoção destas tecnologias pelas empresas portuguesas está a ser mais rápida e intensa que na maioria dos países da União Europeia.

A menor exposição digital das empresas portuguesas, em comparação com a média da União Europeia, reduz os seus riscos cibernéticos. Não obstante, num contexto como o atual, em que os riscos tendem a aumentar mesmo para níveis de exposição relativamente baixos, em Portugal as empresas devem fazer um esforço para melhorar os seus níveis de cibersegurança a curto e médio prazo.

3.3 A SEGURANÇA

A digitalização, em geral, e a expansão das conexões digitais das empresas por motivos de imagem e divulgação (páginas de Internet e redes sociais), de comercialização e fornecimento (páginas de Internet, redes sociais, *apps*, plataformas, IA), de integração de sistemas (ERP, CRM e outros), de gestão de dados (*Big Data*) e de produção e logística (IoT, robótica e IA) estão a impulsionar a adoção de medidas para garantir elevados níveis de cibersegurança nas empresas. A perceção dos riscos cibernéticos tem vindo a aumentar e, consequentemente, as empresas estão mais dispostas a adotar medidas de proteção que evitem disrupções na sua operação e impactos nas suas contas de resultados.

Figura 3.19 – Empresas que utilizam, pelo menos, uma medida de segurança das TIC, 2019, países da UE-27, % de empresas

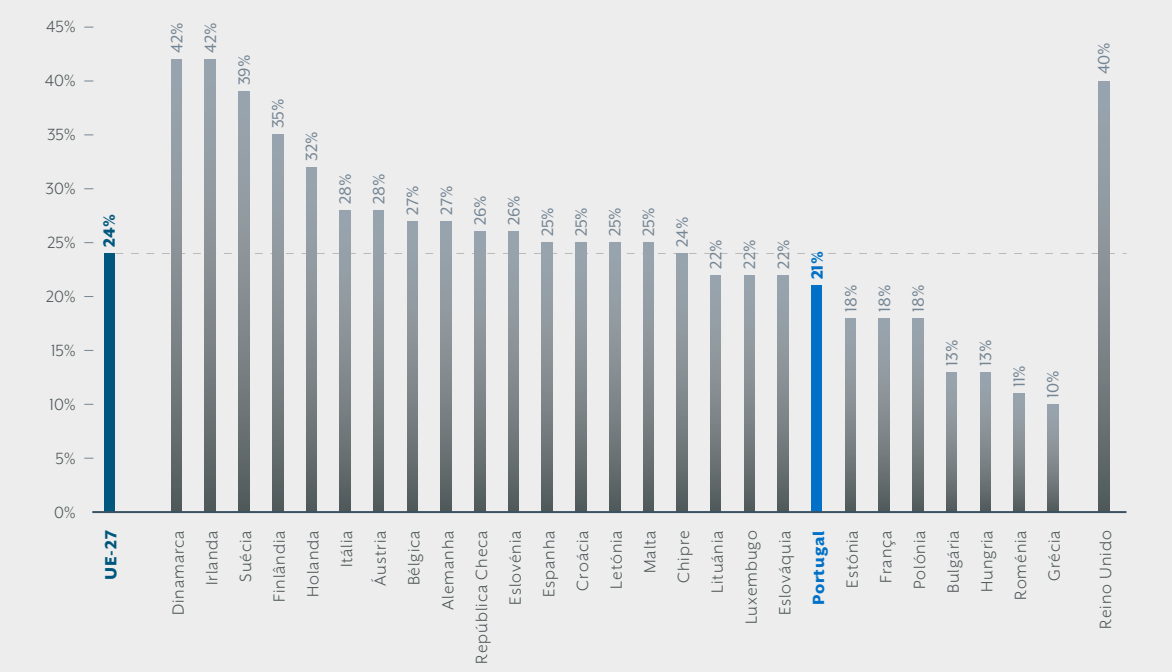


Fonte: Eurostat.

A Figura 3.19 apresenta a percentagem de empresas europeias que, em 2019, utilizavam alguma medida de segurança das TIC.[64] Nesse ano, 92% das empresas europeias (UE-27) empregavam alguma medida de segurança neste âmbito.

Em seis países europeus, mais de 95% das empresas adotaram pelo menos uma medida deste tipo. Neste domínio, Portugal é o segundo país onde mais empresas adotam alguma medida de segurança. Estas práticas estão bastante generalizadas na União Europeia, dado que, mesmo nos países mais atrasados nesta área, três em cada quatro empresas implementam pelo menos uma medida para proteger as suas TIC, embora na maioria dos casos seja manifestamente insuficiente.

Figura 3.20 – Empresas cuja política de segurança das TIC foi definida ou revista pela última vez nos últimos 12 meses, 2019, países da UE-27, % de empresas

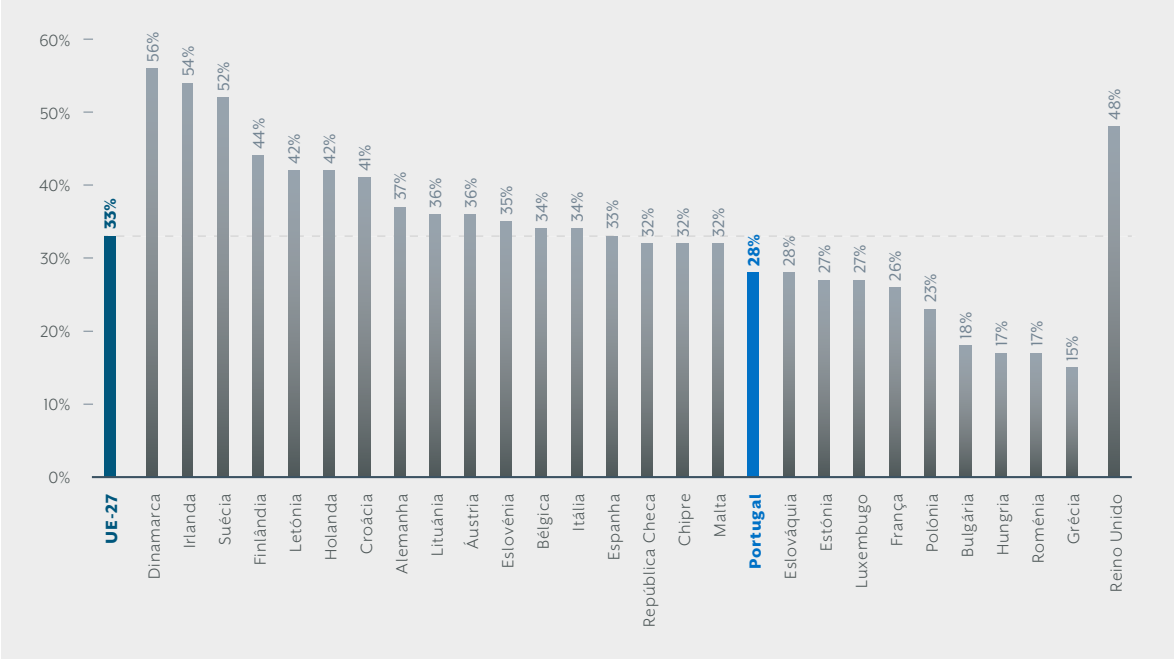


Fonte: Eurostat.

Dada a dinâmica dos riscos cibernéticos, as empresas tendem a definir novas políticas de segurança ou a rever as já existentes cada vez com mais frequência. A Figura 3.20 mostra a percentagem de empresas europeias cuja política de segurança foi definida ou revista no último ano, em 2019. Um quarto das empresas europeias (UE-27) (24%) definiu ou reviu a sua política de segurança nos últimos doze meses. Na Dinamarca e na Irlanda a percentagem é de 42%, enquanto que na Bulgária, na Roménia, na Hungria e na Grécia é inferior a 15%. Em Portugal, pouco mais de uma em cada cinco empresas define ou revê a sua estratégia de segurança com muita frequência (no último ano).

64. Nos gráficos que constam a seguir, os dados dizem respeito ao ano mais recente para o que existem dados. Em muitos casos, só existem dados para 2019. Na maioria dos casos, não existem dados para períodos prévios que, se existirem, permitiriam efetuar comparações inter-temporais.

Figura 3.21 – Empresas europeias que possuem documento(s) sobre medidas, praticas e procedimentos de segurança das TIC, 2019, países da UE-27, % de empresas



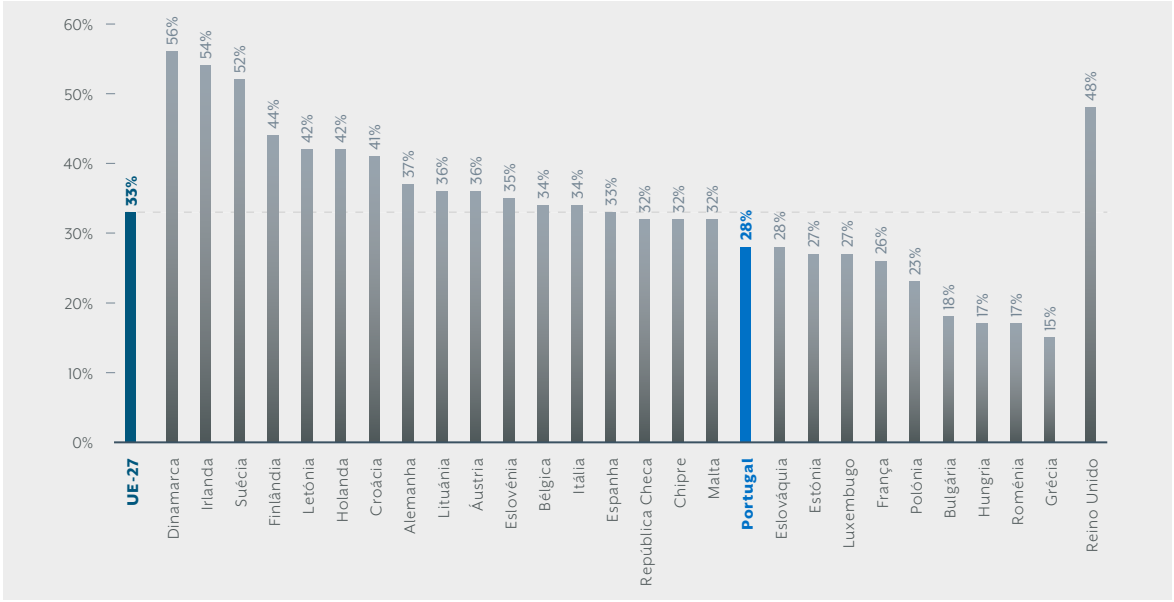
Fonte: Eurostat.

Uma prática que introduz rigor e consistência no âmbito da cibersegurança consiste em documentar a política de segurança da empresa. Na Figura 3.21 apresenta-se a percentagem de empresas europeias que possui documentos sobre medidas, práticas e procedimentos de segurança das TIC.

Uma em cada três empresas europeias (UE-27) tem documentos com os seus protocolos de segurança das TIC. Esta prática é comummente adotada pelas empresas nórdicas, irlandesas e holandesas (entre 42% e 56% das empresas). Tal como no caso anterior, é pouco frequente entre as empresas da Bulgária, da Hungria, da Roménia e da Grécia (entre 15% e 18%). Em Portugal, 28% das empresas têm uma política de segurança documentada.

O esforço das empresas para atualizar a política de segurança com a finalidade de adaptá-la à evolução dos riscos e ameaças cibernéticas pode ser pouco eficaz, em termos de proteção, se os empregados estiverem pouco consciencializados da relevância de cumprir os protocolos de segurança. A Figura 3.22 mostra a percentagem de empresas europeias que procuram que os seus empregados estejam cientes das suas obrigações em matéria de segurança.

Figura 3.22 – Empresas que fazem com que os seus empregados sejam cientes das suas obrigações em matéria de segurança das TIC, 2019, países da UE-27, % de empresas

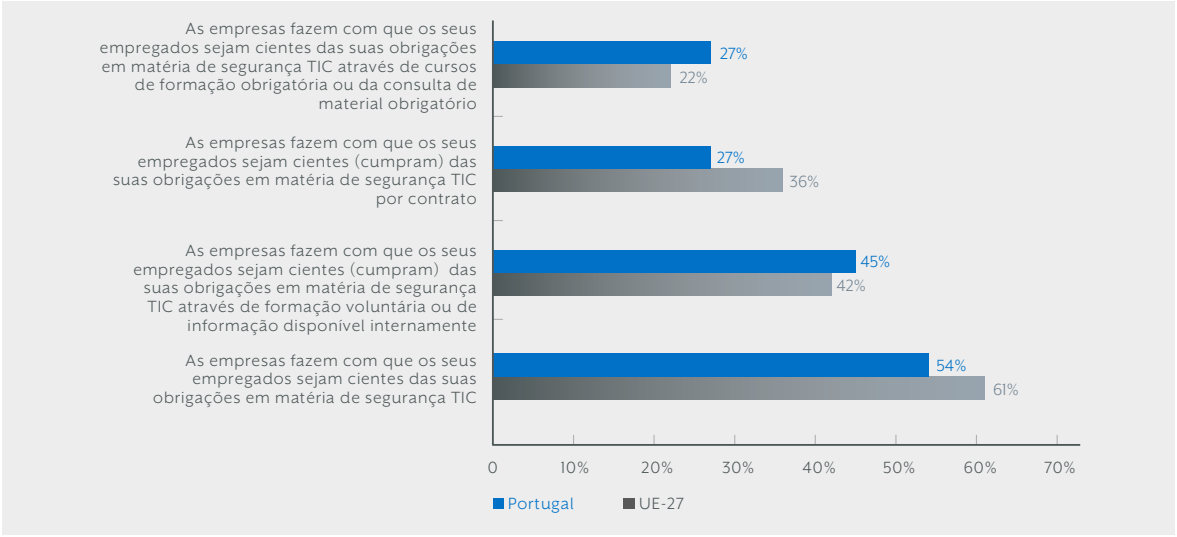


Fonte: Eurostat.

Aproximadamente três em cada cinco empresas europeias (UE-27) têm essa preocupação, sendo que na República Checa, Irlanda e Itália esse cuidado está presente em três em cada quatro empresas. O pior desempenho neste indicador é para a Grécia, onde apenas uma em cada três empresas incutem nos seus trabalhadores esta responsabilidade. Em Portugal, tal como em Espanha, 54% das empresas procuram que os seus empregados conheçam as suas obrigações em matéria de segurança.

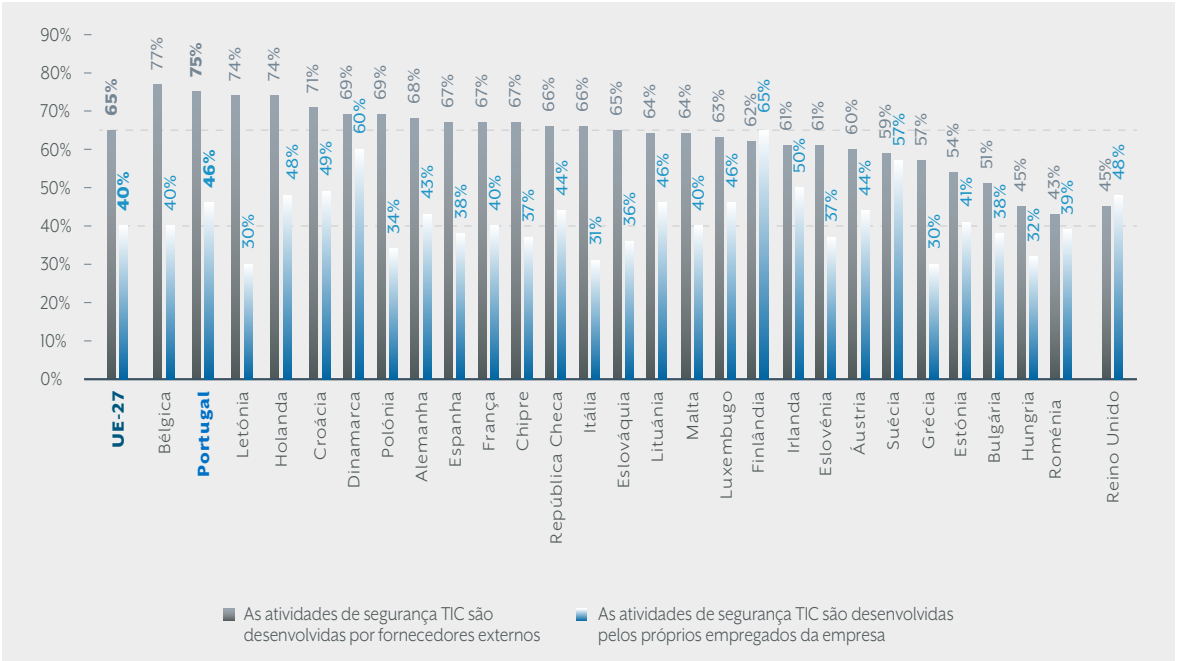
A abordagem das empresas para conseguirem cumprir as suas obrigações em matéria de segurança das TIC pode ser muito diferente. As empresas podem optar por políticas de natureza voluntária, baseadas em orientações, ou por políticas de caráter obrigatório, baseadas em contratos. Na Figura 3.23 apresenta-se a percentagem de empresas que têm esta preocupação e que adotam uma das três principais estratégias possíveis para que os empregados sejam responsáveis no domínio da segurança das TIC, quer em Portugal, quer na União Europeia. Na União Europeia, 42% das empresas procuram fazer com que os seus empregados cumpram as suas obrigações através de cursos de formação voluntária e de consulta de material, 36% mediante obrigações contratuais e 24% obrigando-os a frequentar cursos de formação ou a consultar material sobre a matéria. Em Portugal 45% das empresas optam pela abordagem voluntária, enquanto que 27% recorrem aos contratos e outras 27% a programas de formação obrigatórios.

Figura 3.23 – Abordagens das empresas para que que os empregados cumpram as suas obrigações em matéria de segurança das TIC, 2019, UE-27 | Portugal, % de empresas



Fonte: Eurostat.

Figura 3.24 – Atividades de segurança das TIC nas empresas – empregados próprios *versus* fornecedores externos, 2019, países da UE-27, % de empresa

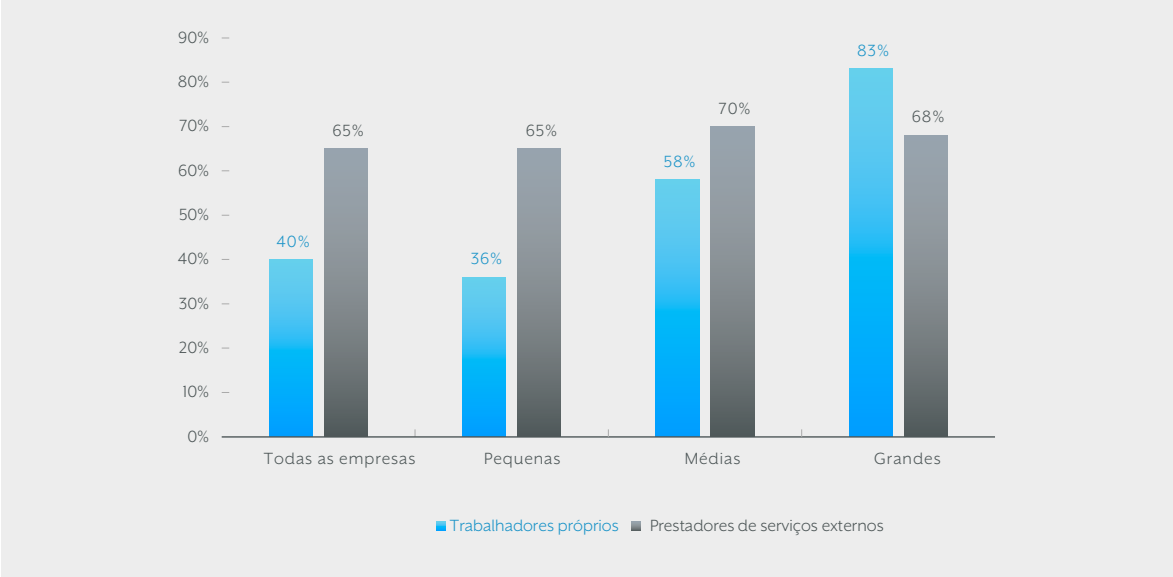


Fonte: Eurostat.

As empresas organizam a sua segurança das TIC de forma diferente. Algumas possuem capacidade interna para desenvolver esta atividade, enquanto outras preferem subcontratá-la. Uma parte considerável segue uma aproximação híbrida, na qual os especialistas internos são apoiados por profissionais externos em algumas tarefas. Na Figura 3.24 apresenta-se a percentagem de empresas europeias que internaliza e/ou externaliza as suas atividades de segurança das TIC, nos vários Estados-membros. Em 40% das empresas europeias (UE-27) a segurança das TIC é efetuada internamente, enquanto 65% delas recorrem a fornecedores externos (em alternativa ou para complementar os recursos internos). Em Portugal, as atividades de segurança das TIC são realizadas por trabalhadores próprios em 46% das empresas, no entanto, 77% delas contratam estes serviços de segurança a outras empresas ou a profissionais de cibersegurança.

A capacidade para internalizar as funções relacionadas com a segurança das TIC nas empresas parece estar correlacionada com a dimensão empresarial. Na Figura 3.25 mostra-se a percentagem de empresas europeias (UE-27) que realizam essas funções internamente ou com recurso a fornecedores externos, segmentadas por tamanho. Mais de 80% das grandes empresas europeias (83%) dispõe de serviços internos de segurança das TIC, enquanto que apenas 58% e 36% das empresas médias e das pequenas, respetivamente, dispõem de trabalhadores próprios dedicados a atividades de segurança das TIC.

Figura 3.25 – Atividades de segurança das TIC nas empresas – empregados próprios *versus* fornecedores externos, em função da dimensão empresarial, 2019, UE-27, % de empresas



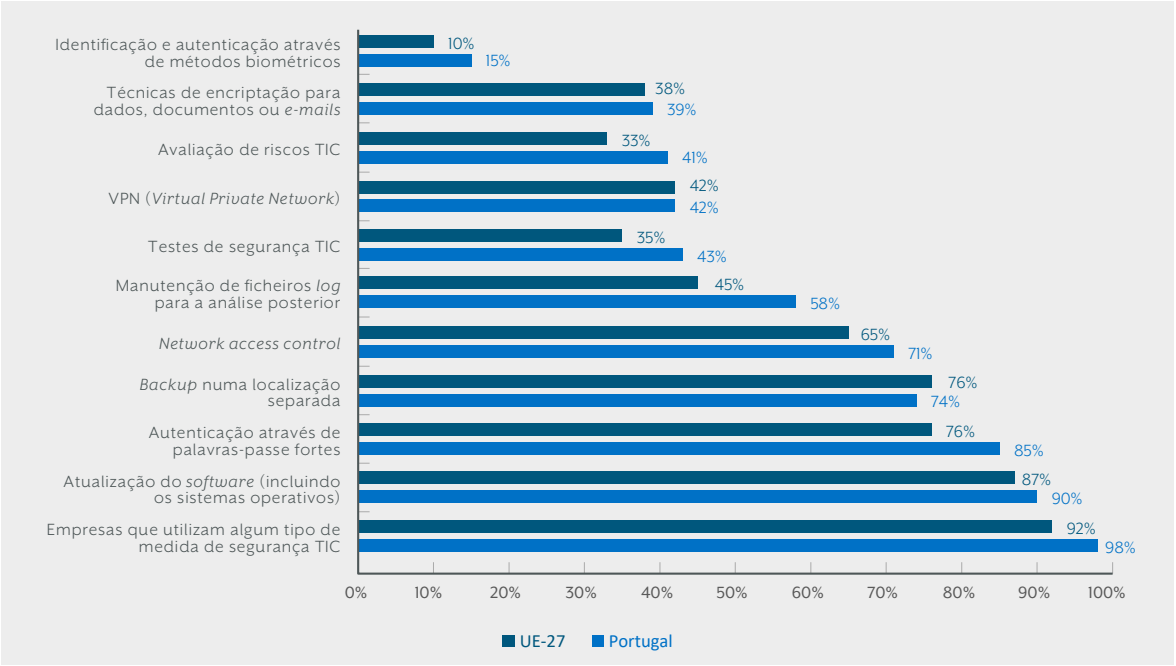
Fonte: Eurostat

No caso dos serviços subcontratados externamente, as diferenças entre empresas de diferentes tamanhos são bastante reduzidas. Aproximadamente dois terços das empresas recorrem a fornecedores externos – 70% das médias empresas, 68% das grandes e 58% das pequenas.

As medidas de segurança das TIC têm evoluído significativamente nos últimos anos, coexistindo atualmente medidas relativamente simples com outras extremamente sofisticadas. Estas últimas, concentram-se em sectores de atividade que gerem informação muito valiosa ou sujeitas a estritas obrigações de privacidade.

A Figura 3.26 apresenta a percentagem de empresas que adota cada uma das medidas de segurança mais frequentes em contexto empresarial, quer na UE-27, quer em Portugal. Em geral, uma maior proporção das empresas portuguesas adota cada uma das medidas elencadas (exceto os *back-ups* numa localização separada). As medidas mais generalizadas, quer na União Europeia, quer em Portugal, são a atualização do *software*, a autenticação através de palavras-passe fortes, os *back-ups* em localizações separadas e o controlo de acesso a redes (*network access control*). As menos frequentes entre as empresas, provavelmente pelo seu grau de sofisticação, são a avaliação de riscos TIC, as técnicas de encriptação de dados e os métodos biométricos de identificação e autenticação.

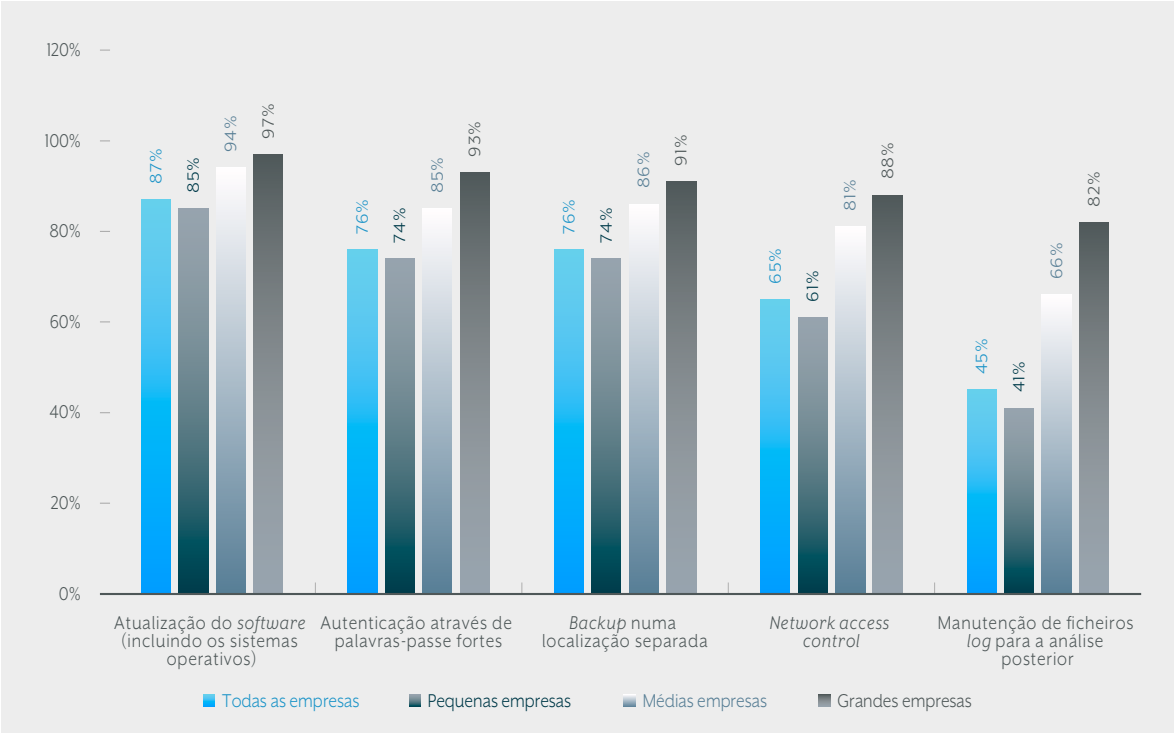
Figura 3.26 – Medidas de segurança das TIC nas empresas, 2019, UE-27 | Portugal, % de empresas



Fonte: Eurostat.

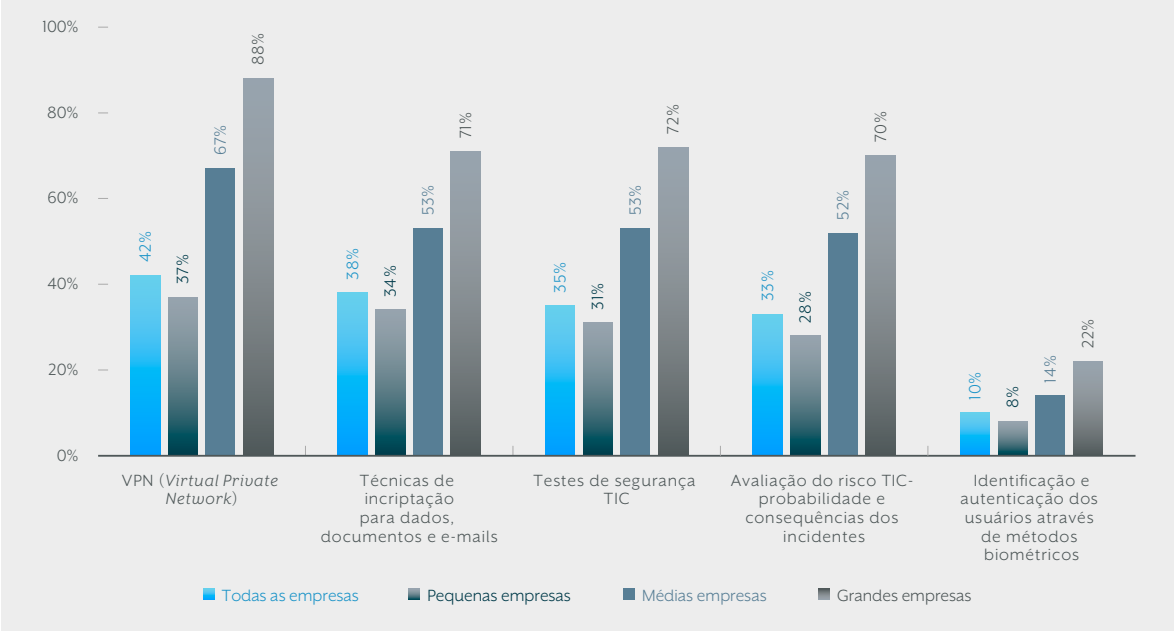
Na Figura 3.27 consta a percentagem de empresas europeias (UE-27) que adota as medidas de segurança mais utilizadas neste âmbito, em função do tamanho empresarial. A Figura 3.28 apresenta o mesmo indicador para as medidas menos utilizadas no domínio empresarial.

Figura 3.27 – Medidas de segurança das TIC mais utilizadas nas empresas, em função da dimensão empresarial, 2019, UE-27, % de empresas



Fonte: Eurostat.

Figura 3.28 – Medidas de segurança das TIC menos utilizadas nas empresas, em função da dimensão, 2019, UE-27, % de empresas

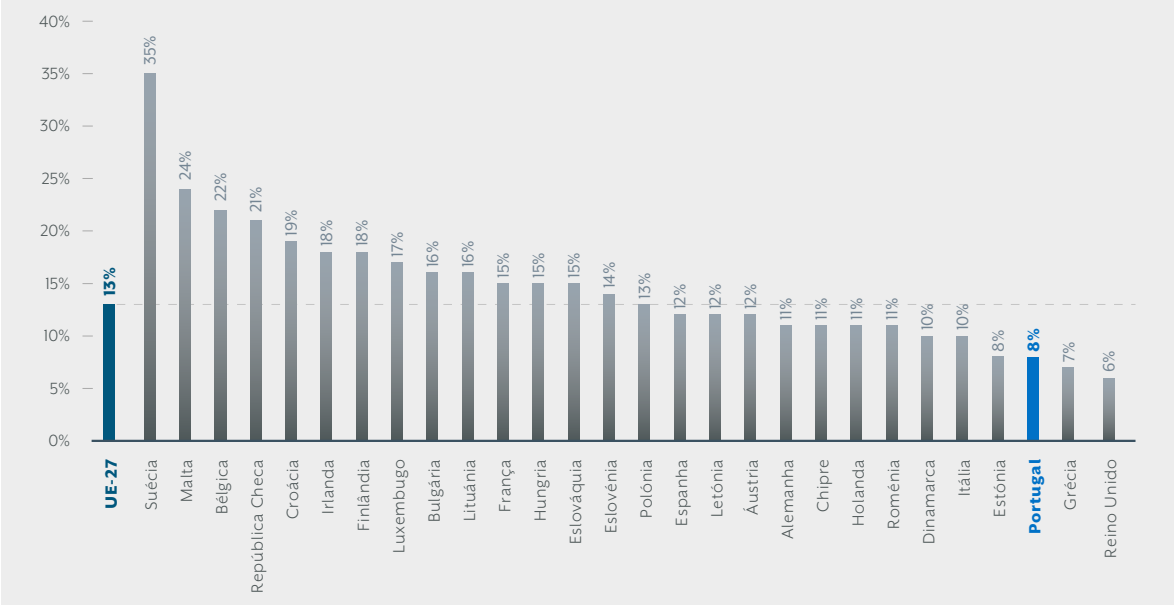


Fonte: Eurostat.

Relativamente às medidas mais frequentes, as diferenças de adoção entre empresas de diversos tamanhos não são muito acentuadas. Contrariamente, nas medidas de segurança menos frequentes, geralmente mais sofisticadas, a adoção por parte das grandes empresas é maior que nas empresas de menor tamanho, em termos relativos. As maiores diferenças em termos de adoção de medidas de segurança entre empresas de diferentes tamanhos verificam-se no caso dos testes de segurança TIC (109% entre pequenas e grandes empresas), das VPN (138%), da avaliação de riscos TIC (150%) e dos métodos biométricos (175%).

Apesar da adoção de medidas de segurança das TIC de maneira cada vez mais generalizada, as empresas continuam a sofrer incidentes de segurança de diversa natureza. Na Figura 3.29 consta a percentagem de empresas europeias (UE-27) que experimentaram, em alguma ocasião, um incidente de segurança. Na União Europeia, 13% das empresas afirma ter experimentado alguma vez um incidente de segurança. O país onde é mais provável que as empresas sofram este tipo de problemas é a Suécia (35% das empresas). Outros países onde mais de uma em cada cinco empresas passou por uma situação desse tipo são Malta, Bélgica e a República Checa. Em Portugal apenas 8% das empresas declara ter sofrido alguma vez este tipo de incidentes, sendo o segundo país onde menos prevalência tem este tipo de episódios no âmbito empresarial – só a Grécia apresenta menor incidência.

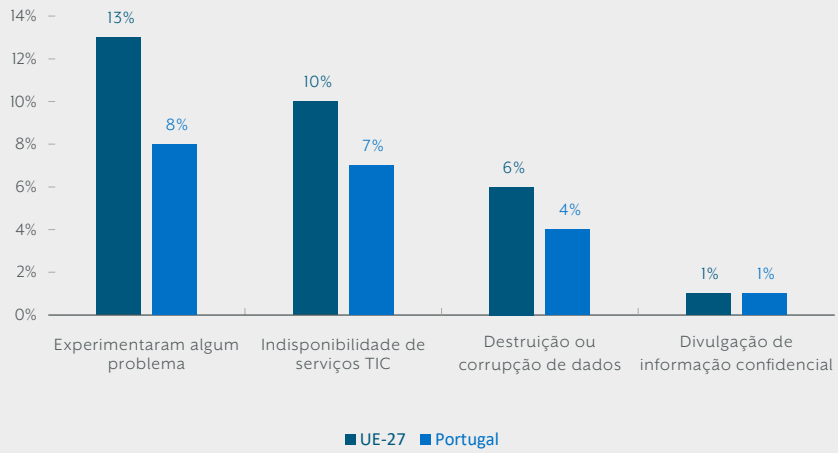
Figura 3.29 – Empresas que experimentaram, pelo menos uma vez, problemas derivados de incidentes de segurança das TIC, 2019, países da UE-27, % de empresas



Fonte: Eurostat.

Os incidentes de segurança que afetam as empresas podem ter naturezas bastante diferentes, o que resulta em consequências para as organizações também diferentes. A Figura 3.30 mostra a percentagem de empresas que experimentaram alguma vez uma das três principais tipologias de incidentes de segurança, na União Europeia e em Portugal. O incidente menos frequente é a divulgação de informação confidencial, dado que apenas 1% das empresas o sofreu em alguma ocasião, tanto no conjunto da União como em Portugal. A destruição ou corrupção de dados afetou alguma vez 6% das empresas da União Europeia e 4% das empresas em Portugal. O incidente mais frequente é a indisponibilidade de serviços TIC, que afeta 10% das empresas europeias (UE-27) e 7% das empresas portuguesas.

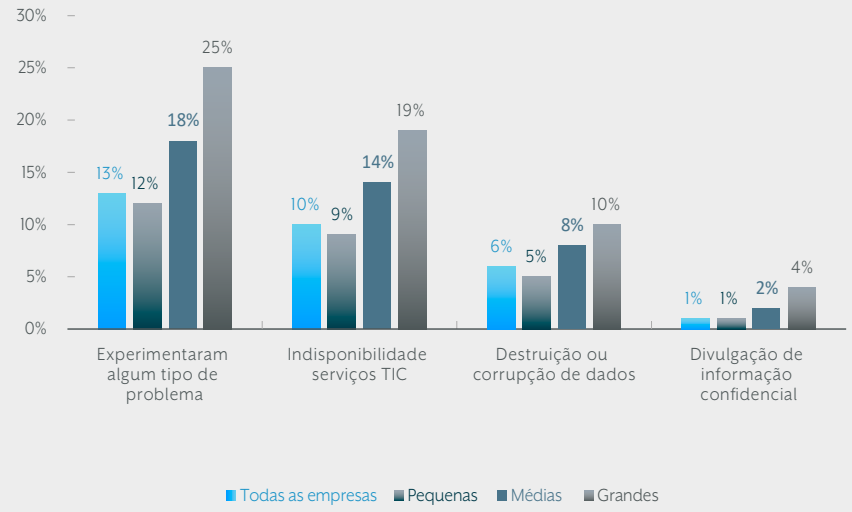
Figura 3.30 – Tipologias de incidentes de segurança das TIC, 2019, UE-27 | Portugal, % de empresas



Fonte: Eurostat.

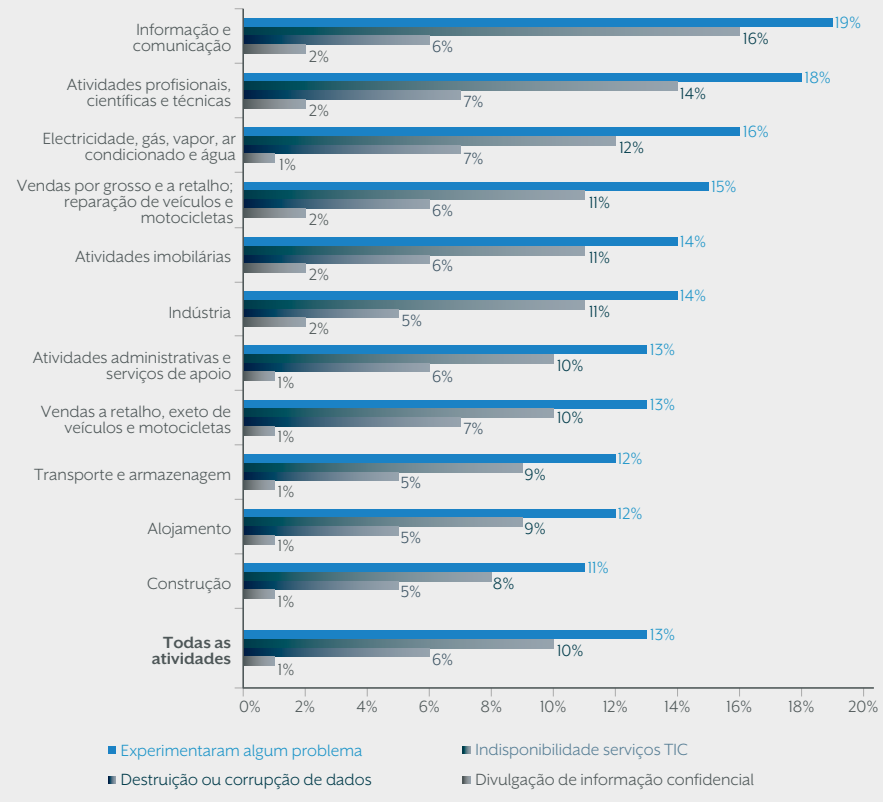
Os incidentes de segurança são mais frequentes à medida que aumenta a dimensão empresarial. Adicionalmente, a tipologia dos incidentes varia em função do tamanho das empresas. A Figura 3.31 mostra a percentagem de empresas europeias (UE-27) que experimentaram um incidente de segurança em função do seu tamanho, assim como por tipologia de incidente. Um quarto das grandes empresas europeias, aproximadamente, um quinto das médias e pouco mais de um oitavo das pequenas sofreu algum incidente de segurança. Observa-se também que existe uma evidente correlação entre tamanho e incidentes, em geral, e por tipologia de incidente.

Figura 3.31 – Tipologias de incidentes de segurança das TIC, 2019, por dimensão empresarial, UE-27, % de empresas



Fonte: Eurostat.

Figura 3.32 – Empresas que experimentaram, pelo menos uma vez, problemas derivados de incidentes de segurança das TIC, por atividade económica, 2019, UE-27, % de empresas



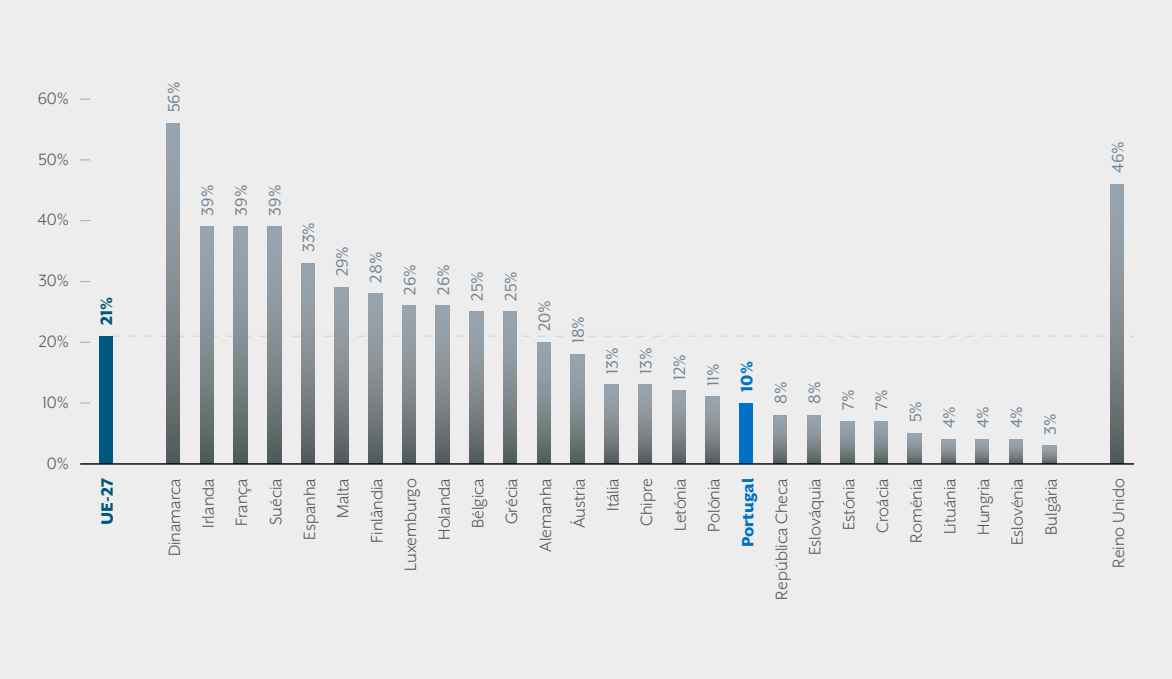
Fonte: Eurostat

Os incidentes de segurança variam consideravelmente por sector de atividade. A Figura 3.32 mostra a percentagem de empresas europeias (UE-27) que sofreram um incidente de segurança por setor de atividade. As empresas mais afetadas por esta problemática são as do sector de informação e comunicação, as de atividades profissionais, científicas e técnicas, as do setor da eletricidade, gás, vapor, ar condicionado e água, assim como as de atividades imobiliárias e as de carácter industrial. As menos afetadas são as dos sectores da construção, o alojamento e o transporte e o armazenamento.

A indisponibilidade de serviços TIC impacta especialmente sobre as mesmas atividades que os incidentes em geral. A destruição e corrução de dados afeta em maior medida as atividades profissionais, o setor da eletricidade, gás, vapor, ar condicionado e água e as vendas a retalho. Os incidentes associados à divulgação de informação confidencial são mais expressivos no setor da informação e da comunicação, nas atividades profissionais, científicas e técnicas, nas vendas por grosso e a retalho, no imobiliário e na indústria.

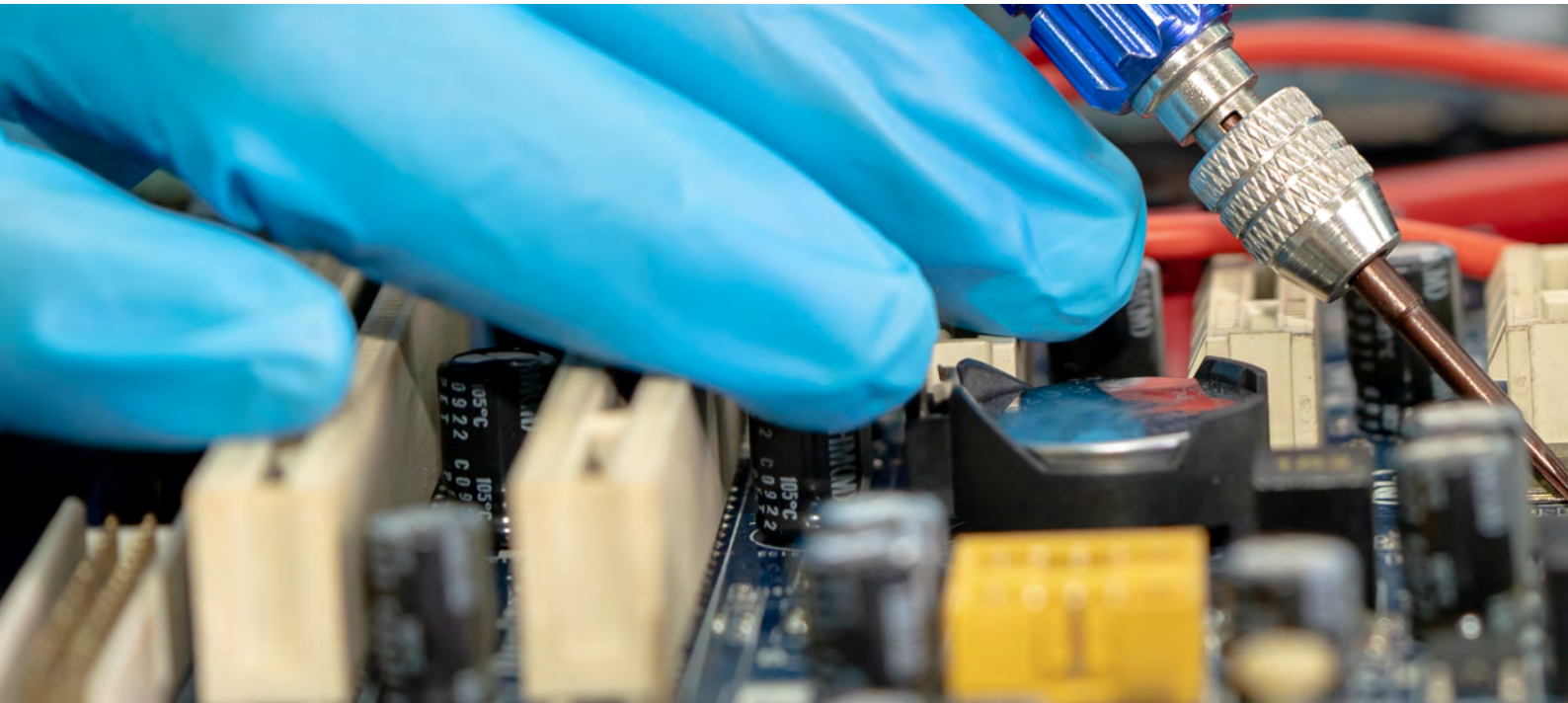
Uma forma de gerir os riscos derivados dos incidentes de segurança é a contratação de seguros para estes fins. Na Figura 3.33 consta a percentagem de empresas europeias que contratam seguros contra incidentes de segurança das TIC. Aproximadamente uma em cada quatro empresas europeias (UE-27) adquirem este tipo de produtos. A Dinamarca é o país líder neste indicador (56% empresas), enquanto que a Bulgária é o mais atrasado dos vinte e sete (3% das empresas).

Figura 3.33 – Empresas que possuem seguros contra incidentes de segurança das TIC, países da UE-27, % de empresas



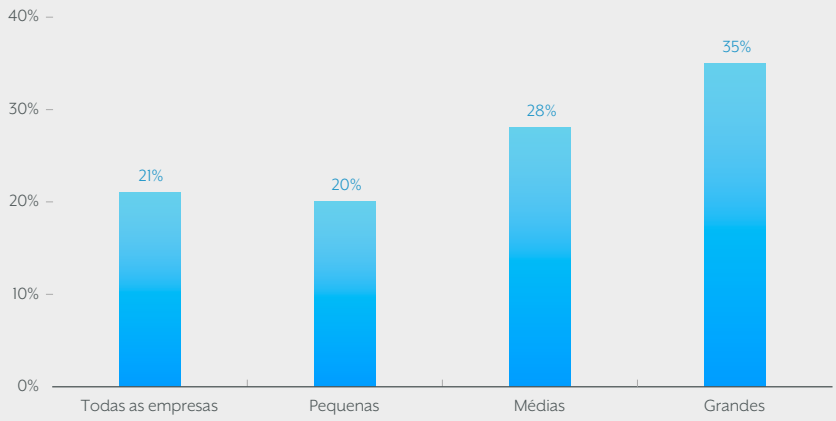
Fonte: Eurostat

Em aproximadamente metade dos países da União Europeia, uma em cada cinco empresas dispõe deste tipo de proteção contra riscos cibernéticos. Em Portugal, essa proporção é bastante inferior, dado que apenas uma em cada dez empresas possuem seguros com este tipo de coberturas.



O tamanho empresarial é relevante para explicar a contratação de seguros contra riscos cibernéticos. Na Figura 3.34 observa-se que, na União Europeia, as empresas de maior dimensão são mais propensas a assegurar-se contra este tipo de riscos. Pouco mais de uma em cada três grandes empresas contrata seguros deste tipo, contra quase três em cada dez no caso das médias e duas em cada dez no caso das pequenas.

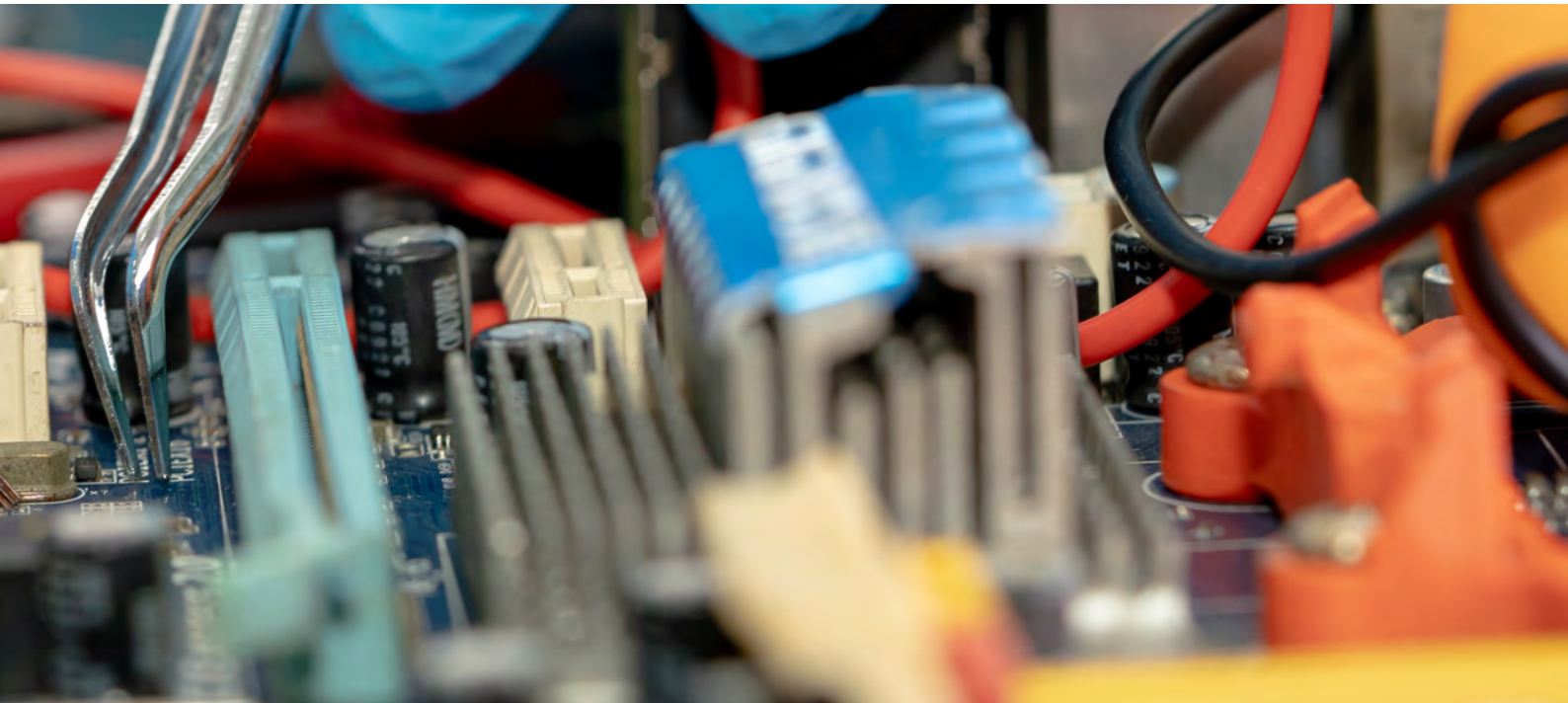
Figura 3.34 – Empresas que possuem seguros contra incidentes de segurança das TIC, UE-27, por dimensão da empresa, % de empresas



Fonte: Eurostat

Em síntese, a maioria das empresas portuguesas dispõe de alguma medida de segurança cibernética, no entanto atualizam-na com pouca frequência, tendem a não formalizar documentalmente as práticas e protocolos de segurança e, em geral, têm dificuldades para sensibilizar os seus empregados sobre a importância da cibersegurança. As medidas de cibersegurança adotadas são similares às das suas congéneres europeias, embora em Portugal exista uma maior prevalência das menos sofisticadas.

Em geral, as empresas portuguesas declaram ter experimentado menos ataques cibernéticos que as empresas de outros países europeus. Esta menor incidência poderá diminuir a perceção dos riscos e, consequentemente, justificar a reduzida adesão das empresas aos seguros contra riscos cibernéticos.



DESTAQUES CAPÍTULO III

O crescimento dos riscos cibernéticos das empresas está associado ao aumento da sua exposição digital. Em geral, as empresas portuguesas apresentam um nível razoável de conectividade digital e uma presença digital desigual. Em relação à média da União Europeia, neste domínio as empresas portuguesas estão ligeiramente atrás, mas genericamente os usos dados aos veículos de visibilização digital são muito similares aos das empresas europeias. Relativamente às vendas *online*, os indicadores das empresas portuguesas são similares aos do conjunto da União, o que não acontece nas compras *online*, onde se situam claramente abaixo. No que se refere ao uso do *Big Data* procedente das interações eletrónicas, bem como de outras fontes, as empresas portuguesas estão abaixo da média comunitária.

Na adoção de sistemas de integração com clientes e fornecedores, as empresas portuguesas estão, em geral, ligeiramente atrás da média da União Europeia, embora existam diferenças entre sistemas. A diferença é maior na incorporação de soluções baseadas em *cloud* computing, onde Portugal surge bastante abaixo da média.

No que se refere à integração de sistemas mais sofisticados, a situação é mista. Por um lado, a incorporação de *robots* industriais e de serviços e sistemas de IA é mais intensa que na maioria dos países da União Europeia, mas, por outro, na adoção de sistemas ou dispositivos interconectados através da Internet (IoT), as empresas portuguesas estão ainda bastante atrás.

Em resumo, nas diversas dimensões que aumentam a exposição digital das empresas – ligação à Internet, presença digital, compras e vendas *online*, interconexão automática com clientes e fornecedores, adoção de sistemas de alojamento remoto e integração de outros sistemas de operação automática/autónoma – e que, consequentemente, potenciam os riscos cibernéticos, as empresas portuguesas estão, todavia, atrás das empresas europeias. Embora esta situação possa ter consequências sobre a competitividade do tecido empresarial português, do ponto de vista da cibersegurança pode ser uma vantagem. A menor exposição digital das empresas portuguesas pode ser aproveitada para melhorar o seu nível de cibersegurança, através de medidas, práticas e protocolos que reduzam o número de incidentes e as suas consequências.

A generalidade das empresas portuguesas dispõe de alguma medida de segurança (em maior medida que na UE-27), mas definem ou reveem a sua política de segurança com pouca frequência e, em geral, não a documentam (em menor medida que na UE-27). Adicionalmente, os seus empregados estão menos consciencializados que a média da União sobre as suas obrigações em matéria de cibersegurança.

As empresas portuguesas combinam a aquisição externa de serviços de cibersegurança, com o desenvolvimento interno deste tipo de funções, embora a opção maioritária seja a externalização. O mesmo acontece a nível europeu (UE-27), mas o nível de sobreposição é inferior. A adquisição de serviços a prestadores externos é transversalmente relevante para empresas de todas as dimensões, mas o desenvolvimento destas funções *in house* é mais frequente à medida que aumenta o tamanho empresarial.

As medidas de segurança das TIC adotadas pelas empresas portuguesas são similares às das empresas europeias (UE-27). Em geral, a intensidade da adoção entre empresas portuguesas é superior às da UE-27, exceto no caso dos *back-ups* em localizações separadas.

A percentagem de empresas portuguesas que afirmam ter sofrido alguma vez problemas derivados de incidentes de segurança das TIC é muito reduzida. Os incidentes mais frequentes, tanto em Portugal como na União Europeia, é a indisponibilidade de serviços de TIC, a destruição ou corrupção de dados e a divulgação de informação comercial. Exceto nesta última tipologia, nas restantes a incidência é maior nas empresas europeias (UE-27) que nas portuguesas.

A contratação de seguros contra riscos cibernéticos por parte das empresas portuguesas é ainda reduzida, se comparada com as suas congéneres europeias (a percentagem de empresas portuguesas com estas coberturas é aproximadamente metade da média da UE-27). Entre as empresas europeias a adesão a estes instrumentos aumenta com a dimensão empresarial.

CAPÍTULO IV
A OFERTA DE CIBERSEGURANÇA EM PORTUGAL
RECURSOS HUMANOS E EMPRESARIAIS

CAPÍTULO IV
A OFERTA DE CIBERSEGURANÇA EM PORTUGAL – RECURSOS HUMANOS E EMPRESARIAIS

4.1 ENQUADRAMENTO

O incremento dos riscos derivados da crescente exposição digital e do aumento da conectividade está a impulsionar a procura de serviços de cibersegurança por parte das empresas portuguesas. Procuram, por um lado, profissionais qualificados para desenvolver as funções de cibersegurança internamente, e, por outro, os serviços de empresas especializadas quando essas funções são alvo de externalização. Por sua vez, essas empresas especializadas, que prestam serviços de cibersegurança, procuram profissionais para criar e reforçar as suas equipas.

O aumento da procura de profissionais deve ir acompanhado de aumentos de oferta. O sistema de ensino deve contribuir para a formação de profissionais em TIC, que possam especializar-se em cibersegurança quer no próprio sistema, quer nas empresas. O mercado de trabalho tem que ser suficientemente flexível para garantir a transferência de profissionais em TIC, de áreas excedentárias pouco dinâmicas, para áreas deficitárias com elevado potencial de crescimento. Igualmente, a entrada de novos prestadores de serviços no mercado de cibersegurança e a reciclagem de outros, tradicionalmente dedicados a outras atividades, são fundamentais para assegurar uma oferta que acompanhe a evolução da procura.

A principal finalidade deste capítulo é quantificar e caracterizar a oferta de cibersegurança em Portugal, quer ao nível dos recursos humanos, quer ao nível dos prestadores de serviços. Para conhecer a oferta de recursos humanos analisa-se a produção de diplomados em TIC e a dotação de profissionais nessa área, por constituírem as principais fontes de recrutamento potencial para desempenhar funções e prestar serviços na área da cibersegurança. Para caracterizar os profissionais de cibersegurança em Portugal são apresentados os resultados de um inquérito realizado pela AP2SI, com o apoio do Observatório de Cibersegurança do CNCS. A fim de dimensionar e caracterizar o sector da cibersegurança em Portugal, constituído pelas empresas que prestam serviços de cibersegurança, é realizado um exercício de seleção e quantificação, recorrendo à Base de Dados *ORBIS EUROPE*.

O resto do capítulo organiza-se em três secções. Na secção dois caracteriza-se a oferta de recursos humanos em TIC – diplomados e profissionais. A caracterização dos profissionais de cibersegurança, realizada com base no inquérito da AP2SI, é apresentada na secção três. Por último, na secção quatro delimita-se e caracteriza-se o sector da cibersegurança em Portugal.

4.2. RECURSOS HUMANOS EM TIC EM PORTUGAL

Para determinar a oferta potencial de profissionais de cibersegurança em Portugal convém conhecer a disponibilidade de diplomados na área das TIC e o número de profissionais que trabalham nesta área. A evolução do número de diplomados permite saber se o sistema de ensino está a produzir futuros profissionais a um ritmo suficiente para cobrir a procura potencial. A oferta de profissionais que trabalham na área das TIC é um indicador importante para aferir se o mercado dispõe de recursos humanos qualificados suficientes para dar resposta às necessidades do mercado, em geral, e da área da cibersegurança, em particular – eventualmente, mediante transferências entre áreas. Na primeira subsecção é apresentada a evolução dos diplomados no ensino superior português, com o grau de licenciado, mestre ou doutor, nas áreas das TIC e é realizada uma comparação com a situação noutros países europeus neste âmbito. A segunda subsecção caracteriza o emprego dos profissionais de TIC, nomeadamente o seu peso no emprego total, a sua evolução temporal e a sua estrutura etária.

4.2.1 DIPLOMADOS EM TIC

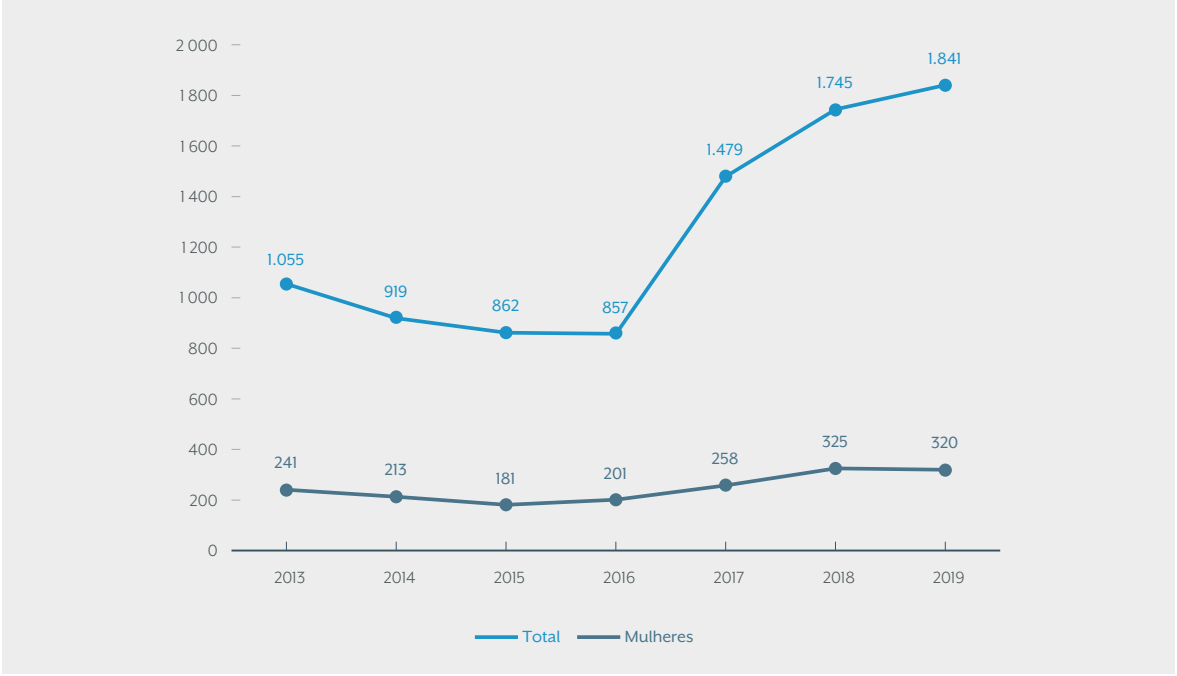
O número de diplomados em TIC em Portugal cresceu de forma significativa, cerca de 75% no período que medeia entre 2013 e 2019, um valor muito acima do crescimento do número de diplomados em todas as áreas (+2,8%) (Figura 4.1). Esta evolução demonstra o considerável esforço do sistema de ensino superior português para dar resposta à crescente procura de profissionais nesta área.[65]

Entre 2013 e 2019, o crescimento do número de mulheres diplomadas em TIC em Portugal foi de 32,8%, inferior ao crescimento médio de diplomados na área. Em 2019, as diplomadas em TIC representavam pouco mais de 17% do total de diplomados, acentuando-se a desigualdade de género na composição dos recursos humanos com qualificação superior passível de ingressarem em atividades de cibersegurança.

65. Embora existam dados de 2020 para Portugal, dado que ao longo da secção são estabelecidas comparações com outros países europeus, recorrendo a dados da Eurostat, por questões de consistência utilizam-se dados desta fonte para o último ano para o que existem dados (2019).

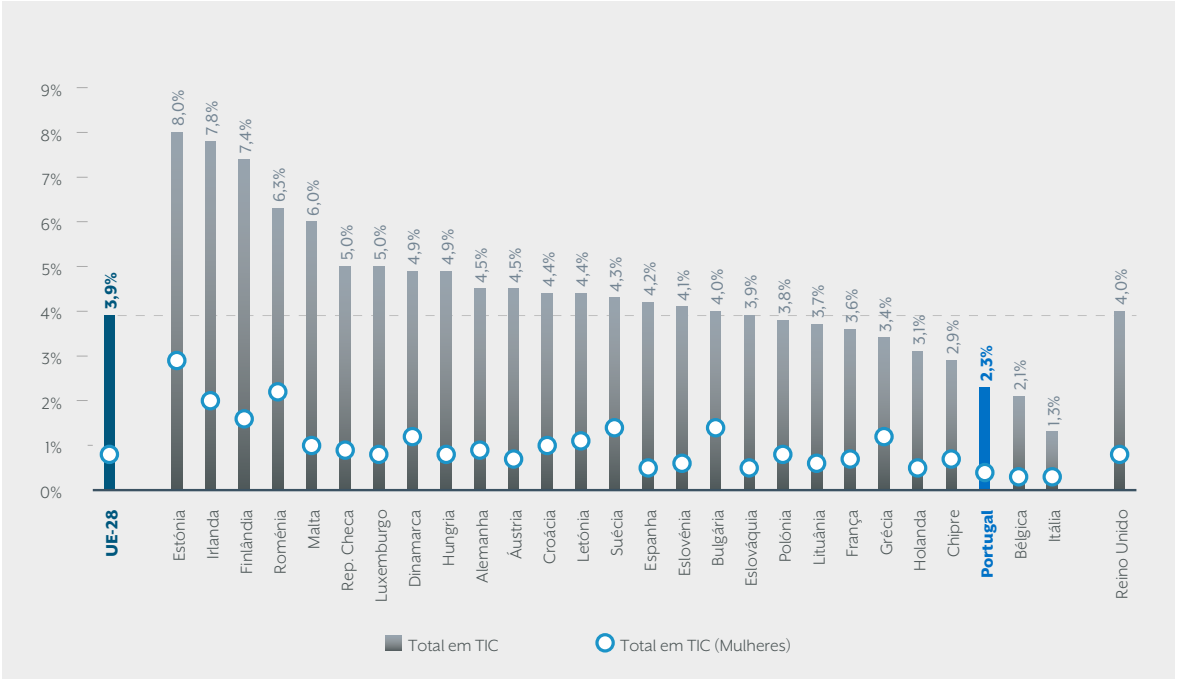
A percentagem de diplomados em TIC em Portugal é a terceira mais baixa da União Europeia, apenas acima da percentagem da Bélgica e de Itália (Figura 4.2). Em 2019, apenas 2,3% dos diplomados no ensino superior português era da área das TIC, um valor abaixo da média europeia de 3,8%, e muito abaixo de países como a Estónia (8,0%) ou a Irlanda (7,8%), que lideram em termos europeus. Relativamente às mulheres diplomadas em TIC no total das diplomadas, estes países ocupam o top três, na primeira e na terceira posição, conjuntamente com a Roménia que ocupa o segundo lugar.

Figura 4.1 – Diplomados no ensino superior em TIC, 2013-2019, Portugal, número de diplomados



Fonte: Eurostat

Figura 4.2 – Diplomados no ensino superior em TIC, 2019, países da UE-28, % do total de diplomados no ensino superior



Fonte: Eurostat

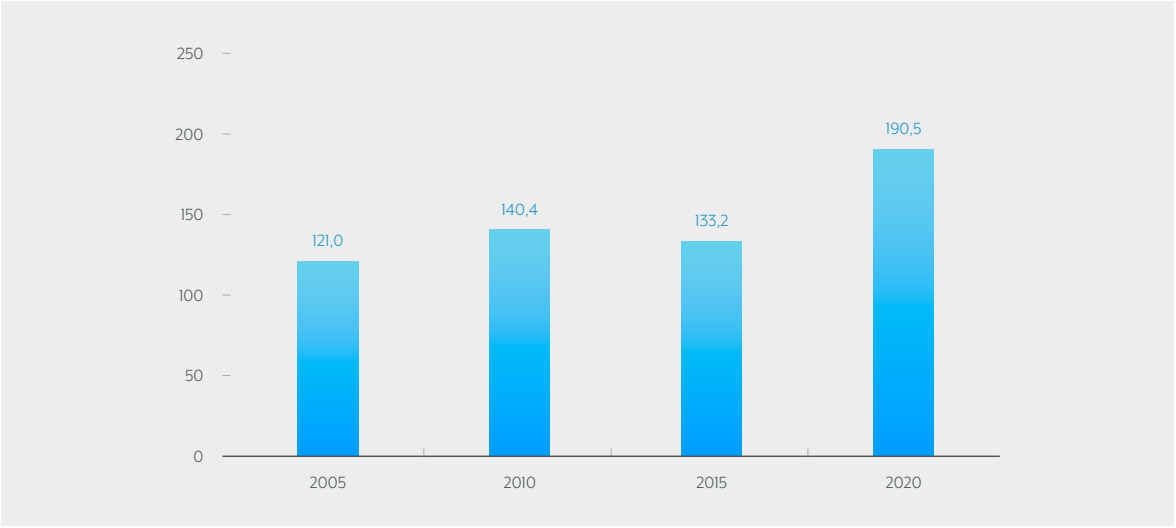
4.2.2 PROFISSIONAIS EM TIC

Entre 2005 e 2020 o número total de especialistas em TIC empregados em Portugal cresceu em 69,5 mil efetivos, para 190,5 mil, um crescimento de 57,4%. De referir que esta variação não foi constante ao longo do período analisado, tendo acelerado nos últimos cinco anos, quando o número de empregados em TIC aumentou em 57,3 mil efetivos (Figura 4.3).

O peso do emprego de especialistas em TIC no emprego total aumentou de 3,0% em 2015 para 4,0% em 2020, aproximando-se da média dos países da União Europeia (4,3%) (Figura 4.4). Portugal é o 16º país da União Europeia a 27 com maior proporção de especialistas em TIC no emprego total. Embora esteja perto da média da União, Portugal encontra-se a uma distância considerável de países como a Finlândia ou a Suécia, onde a percentagem de especialistas em TIC no emprego total é próxima de 8% (7,6% e 7,5%, respetivamente).

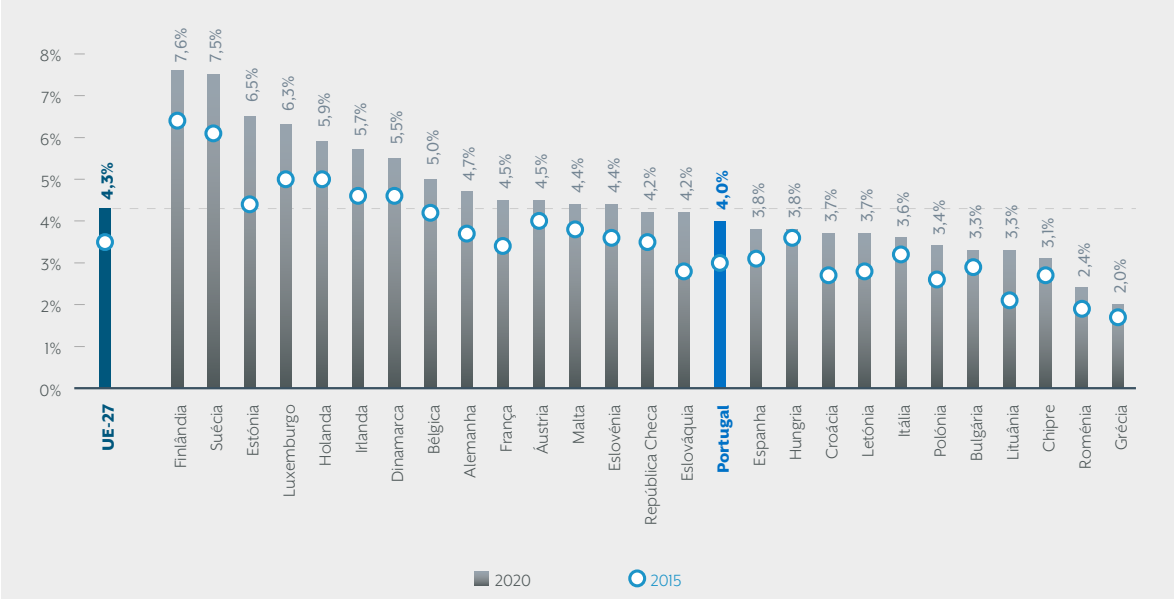
Em Portugal, a percentagem de especialistas em TIC com idade inferior a 35 anos no total de especialistas nessa área é superior à média da União Europeia (38,9% versus 36,4%) (Figura 4.5). No entanto, nos últimos cinco anos verificou-se uma descida desse rácio, passando de 40,1% em 2015 para os 38,9% em 2020. Embora esta tendência seja comum a vários países europeus, em média, o peso dos especialistas jovens no sector permaneceu estável (36,4% na UE-27). A perda de peso do grupo de idade mais jovem entre os especialistas em TIC em Portugal denota o progressivo envelhecimento dos recursos humanos do sector (Figura 4.5).

Figura 4.3 – Emprego de especialistas em TIC, 2005-2020, Portugal, milhares de especialistas



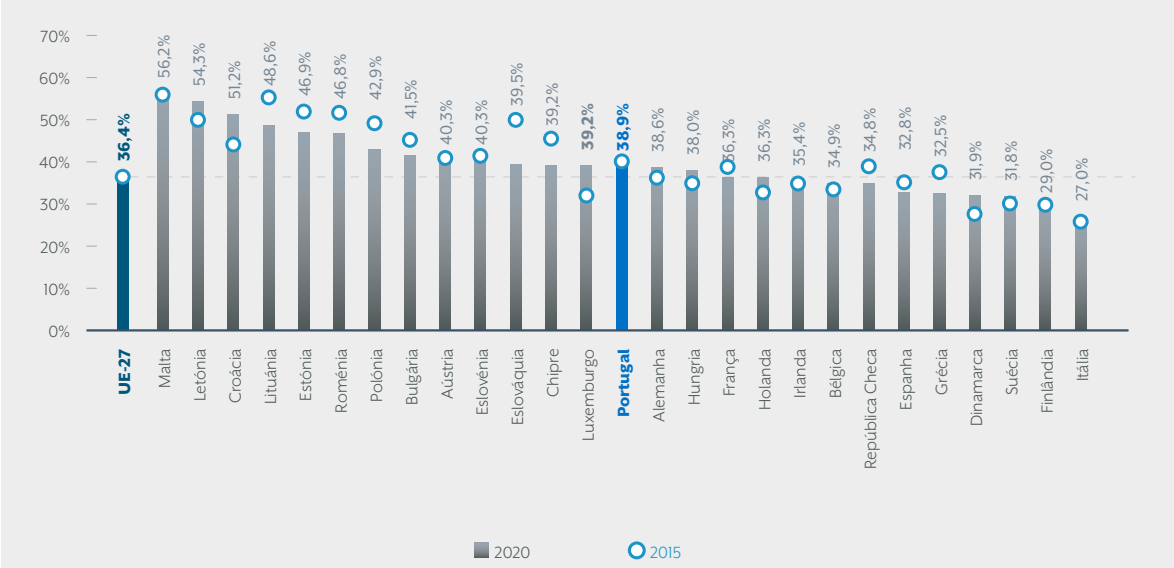
Fonte: Eurostat

Figura 4.4 – Emprego de especialistas em TIC, 2020|2015, países da UE-27, % do emprego total



Fonte: Eurostat

Figura 4.5 – Emprego de especialistas em TIC, 2020|2015, países da UE-27, % de empregados dos 15 aos 34 anos



Fonte: Eurostat

4.3. OS PROFISSIONAIS DE CIBERSEGURANÇA EM PORTUGAL

Esta secção sistematiza os resultados de um inquérito aplicado pela AP2SI, com o apoio do Observatório de Cibersegurança do CNCS, sobre os profissionais de cibersegurança e segurança da informação em Portugal. O inquérito foi aplicado entre os dias 20 e 30 de setembro de 2021, em formato *online*, aberto e anónimo. Foram obtidas 330 respostas completas.

As questões incluídas no inquérito tinham como objetivos caracterizar demograficamente os profissionais e conhecer a sua situação profissional e a sua empregabilidade passada e atual, bem como obter informação sobre os fatores que, no seu entendimento, são relevantes para desenvolver a sua atividade profissional.

4.3.1 CARACTERIZAÇÃO DEMOGRÁFICA

Um quinto dos profissionais da cibersegurança (20,3%) tem 30 anos ou menos e quase metade (47%) 40 anos ou menos (Figura 4.6).[66] Quase quatro em cada dez profissionais deste ramo de atividade (39,7%) têm entre 41 e 50 anos. Face aos resultados de 2019,[67] observa-se certa estabilidade entre as faixas etárias extremas (20 anos ou menos e 51 anos ou mais) e uma redistribuição entre as faixas etárias centrais, dado que a percentagem de respondentes entre 41 e 50 anos aumentou e a de entre 31 e 40 anos diminuiu, o que revela certo envelhecimento da amostra.

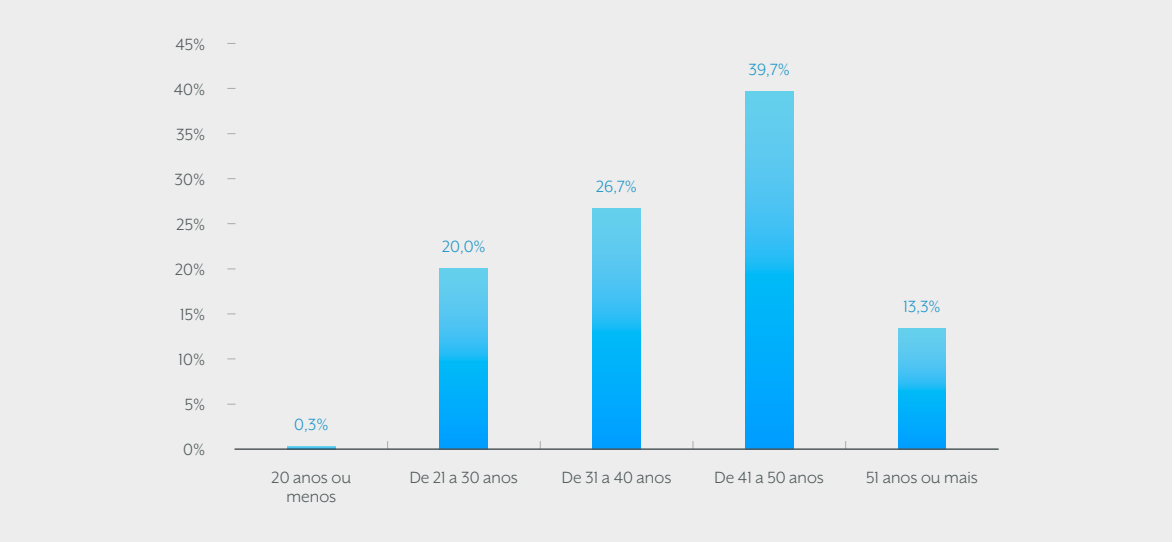
A larga maioria dos profissionais são do sexo masculino (84,2%), refletindo a baixa percentagem quer de diplomados quer de empregados do sexo feminino na área das TIC (Figura 4.7). Contudo a participação das mulheres no sector da cibersegurança (13,4%) é inferior à proporção de diplomadas em TIC (17,4%). No entanto, o peso das profissionais do sexo feminino aumentou face ao inquérito de 2019, onde era de apenas 9%.

Em termos de qualificações, a generalidade dos profissionais tem como habilitação académica mínima o ensino superior (83,0%); deles, dois terços possuem doutoramento ou uma licenciatura pré-Bolonha ou um mestrado (4,2% e 52,1%, respetivamente) (Figura 4.8). Apenas 17,0% dos profissionais apresentam um nível de qualificação inferior ao superior.

66. Embora não seja possível estabelecer uma comparação com a estrutura de idades dos especialistas em TIC, dado que os grupos de idade são diferentes, parece que a proporção dos profissionais jovens no total de profissionais, quer dos especialistas em TIC, quer dos especialistas em cibersegurança é relativamente similar (especialistas em TIC, entre 15 e 34 anos, 38,9%, e especialistas em cibersegurança, com 40 anos ou menos, 47%).

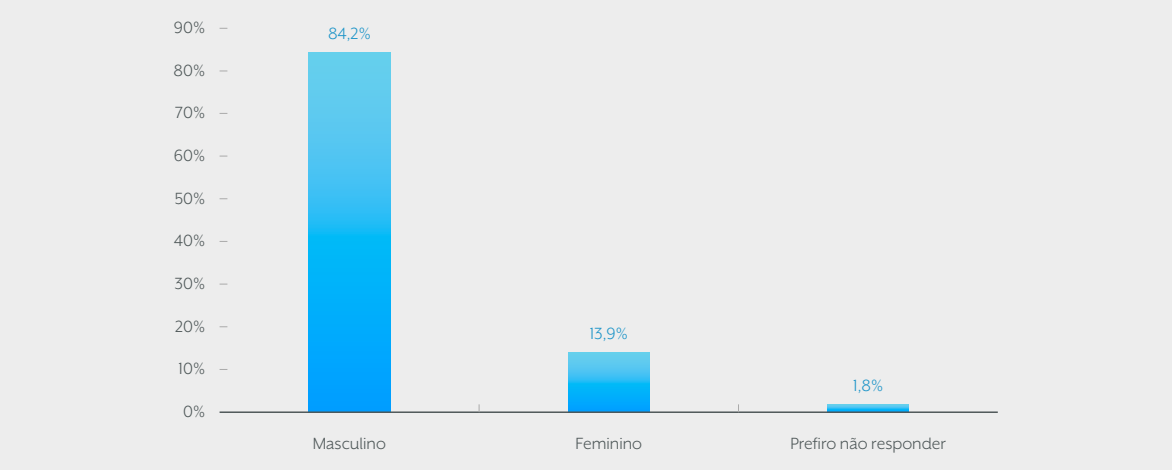
67. A AP2SI realizou um inquérito similar em 2019, que serve como elemento de comparação com os resultados de 2021.

Figura 4.6 – Idade dos profissionais de Cibersegurança



Fonte: Inquérito AP2SI aos profissionais de Cibersegurança

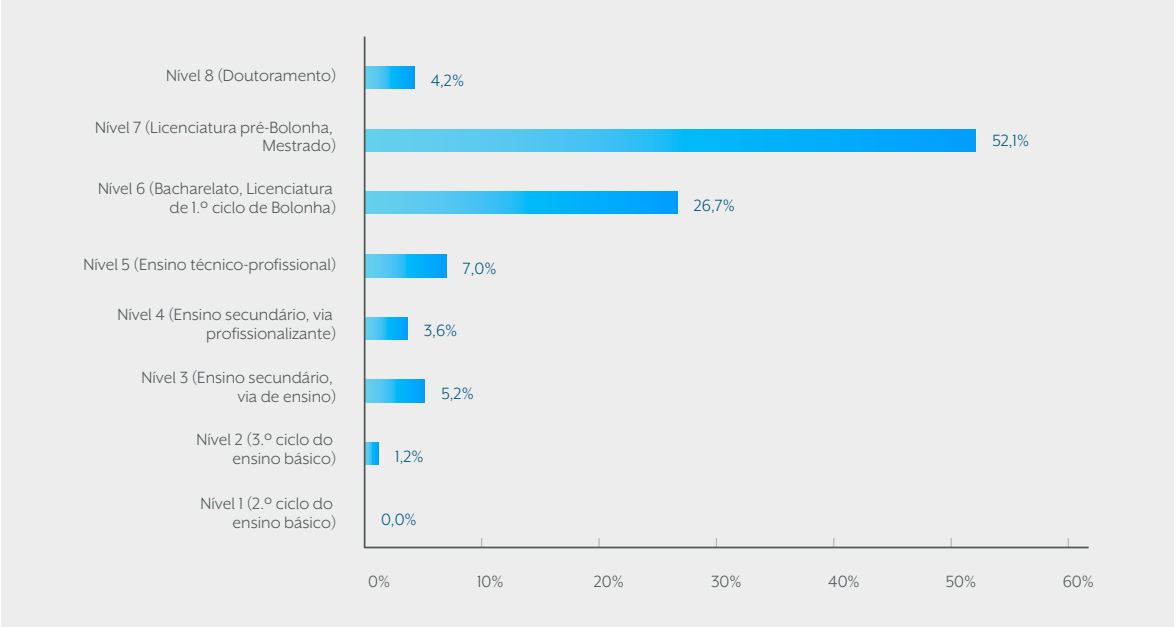
Figura 4.7 – Género dos profissionais de Cibersegurança



Fonte: Inquérito AP2SI aos profissionais de Cibersegurança

Face ao inquérito de 2019, a principal alteração é o aumento dos profissionais com formação de nível 6, provavelmente com licenciatura, e a redução dos que possuem formação de nível 5, ou seja, cursos de ensino técnico-profissional. Esta alteração indicia que uma parte dos profissionais com cursos de nível 5 completaram cursos de nível 6 nos últimos dois anos. Ou seja, genericamente, pode concluir-se que neste período houve um reforço da formação de base dos profissionais de cibersegurança.

Figura 4.8 – Qualificações dos profissionais de Cibersegurança



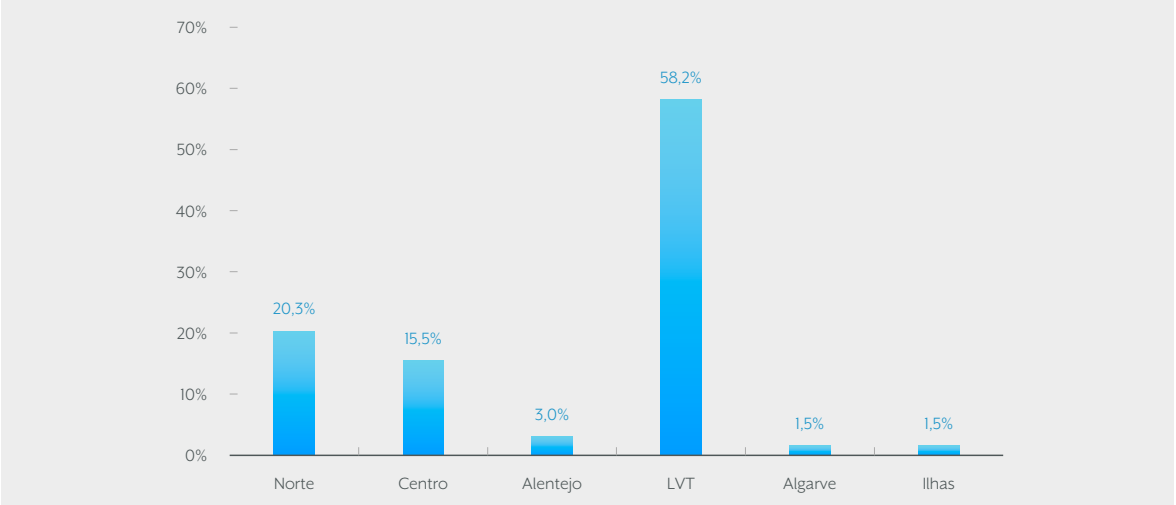
Fonte: Inquérito AP2SI aos profissionais de Cibersegurança

4.3.2 CARACTERIZAÇÃO PROFISSIONAL

A região de Lisboa e Vale do Tejo (LVT) concentra quase seis em cada dez profissionais (58,2%) (Figura 4.9). Nas regiões Norte e Centro desenvolvem a sua atividade pouco mais de um terço dos profissionais (35,8%). Nas restantes regiões estão localizados apenas 6,0% dos profissionais. Face ao inquérito de 2019, verifica-se um reforço da atratividade para estes profissionais da região de Lisboa e Vale do Tejo e da região Centro e algum retrocesso da região Norte.

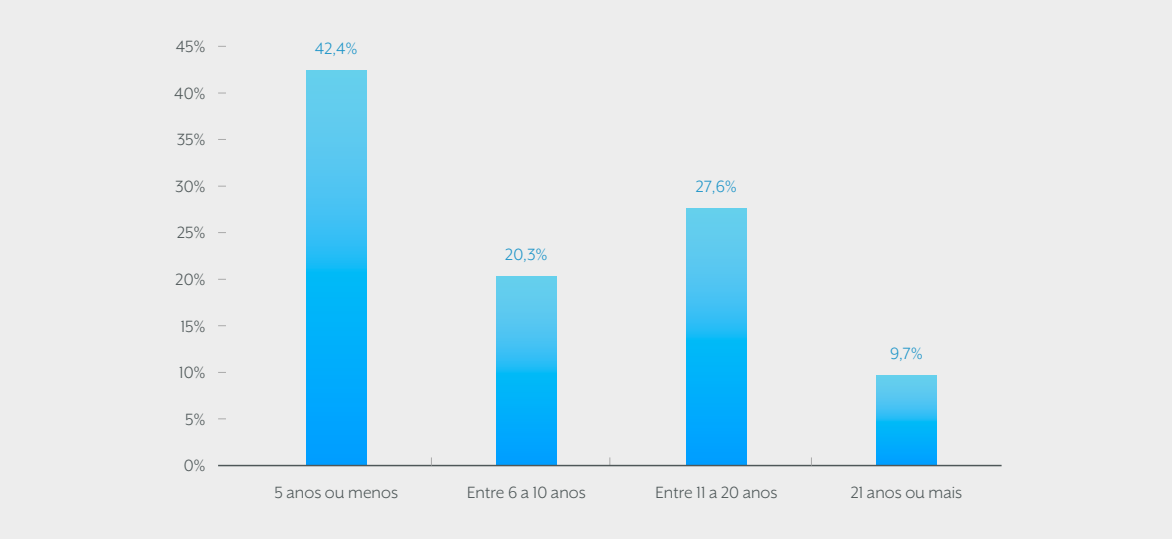
Quase dois terços dos profissionais (62,7%) têm até dez anos de experiência, mais de um quarto (27,6%) entre onze e vinte anos de experiência e quase um décimo (9,7%) mais de vinte anos de experiência (Figura 4.10). Dos que possuem dez anos de experiência ou menos, mais de dois terços (67,6%) tem cinco anos de experiência ou menos. No inquérito de 2019, a percentagem de profissionais com menos de dez anos de experiência era de 70% e com entre onze e vinte anos de experiência de 21%. Desta forma, observa-se um aumento da experiência dos profissionais de cibersegurança, à medida que amadurece o sector. Apesar da importância que a experiência pode ter para enfrentar a complexidade crescente dos incidentes de cibersegurança, convém que o sector continue a beneficiar da entrada de profissionais novos, bem formados e com competências diferenciais e diversificadas.

Figura 4.9 – Regiões onde os profissionais de Cibersegurança desenvolvem a sua atividade



Fonte: Inquérito AP2SI aos profissionais de Cibersegurança

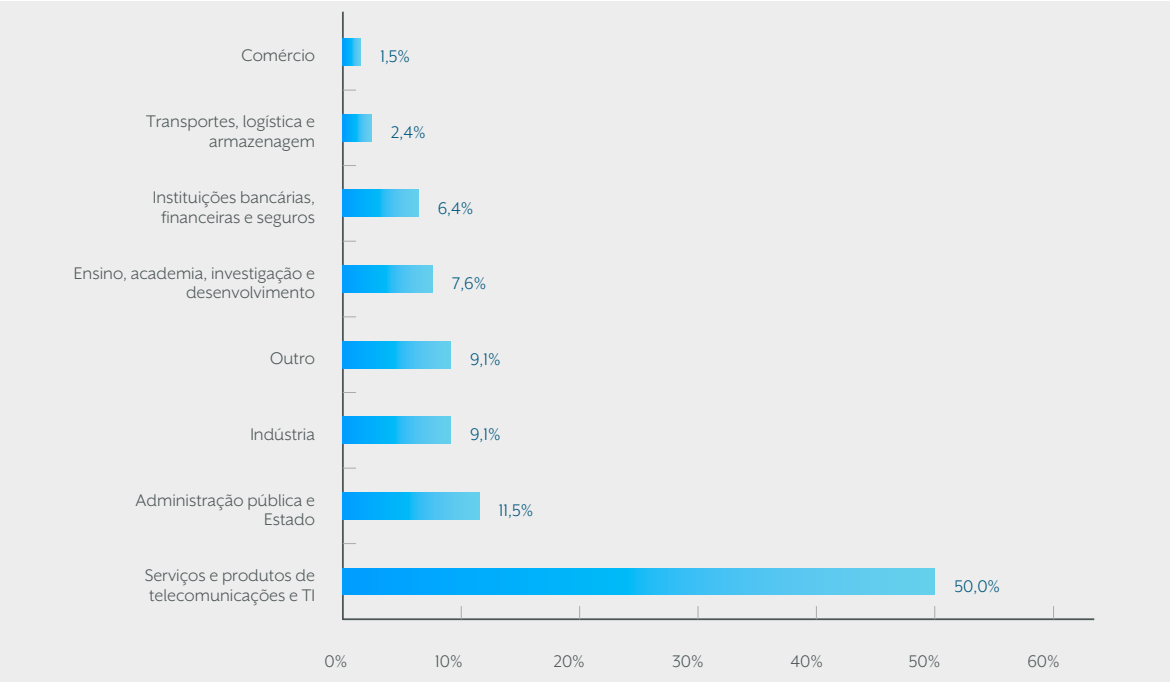
Figura 4.10 – Experiência dos profissionais de Cibersegurança



Fonte: Inquérito AP2SI aos profissionais de Cibersegurança

Metade dos profissionais (50,0%) desenvolve a sua atividade no sector dos Serviços e produtos de telecomunicações e tecnologias de informação e quase um em cada dez (11,5%) na Administração Pública e Estado (Figura 4.11). A Indústria, o Ensino, academia, investigação e desenvolvimento e as Instituições bancárias, financeiras e seguros são também sectores relevantes em termos de emprego, empregando entre 6% e 9% dos profissionais. Em relação ao inquérito de 2019, verifica-se um reforço significativo (+10 p.p.) dos profissionais que desenvolvem a sua atividade no sector de Serviços e produtos de telecomunicações e tecnologias de informação e uma perda de importância da Administração Pública e Estado, e, em menor medida, da Indústria, o Ensino, academia, investigação e desenvolvimento e as Instituições bancárias, financeiras e seguros.

Figura 4.11 – Sectores onde os profissionais de Cibersegurança desenvolvem a sua atividade

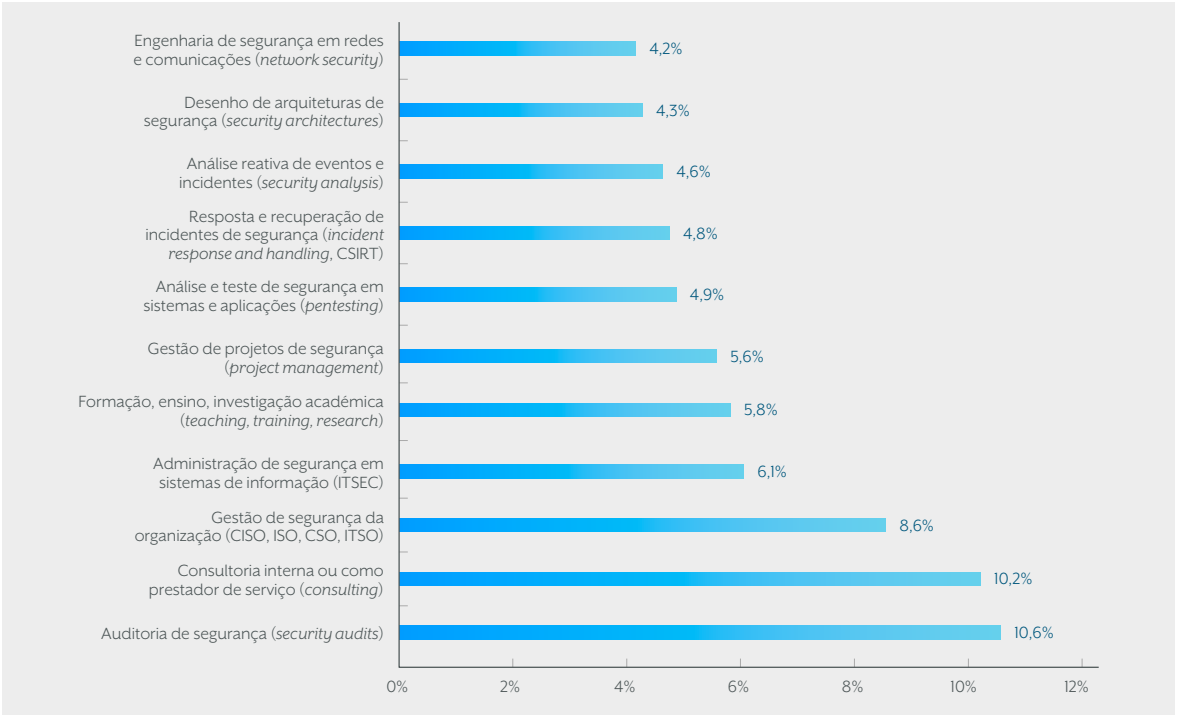


Fonte: Inquérito AP2SI aos profissionais de Cibersegurança

A principal atividade desenvolvida pelos profissionais de cibersegurança é a de Auditoria de segurança (10,6%), seguida da Consultoria interna ou prestação de serviços (10,2%), a Gestão de segurança da organização (8,6%) e a Administração de segurança em sistemas de informação (6,1%) (Figura 4.12). Embora com menor importância, são de referir as atividades de Formação, ensino, investigação académica e de Gestão de projetos de segurança. Para além das tarefas e atividades mais comuns, os profissionais de cibersegurança também levam a cabo outras atividades, embora sejam bastante menos frequentes (Figura 4.13).

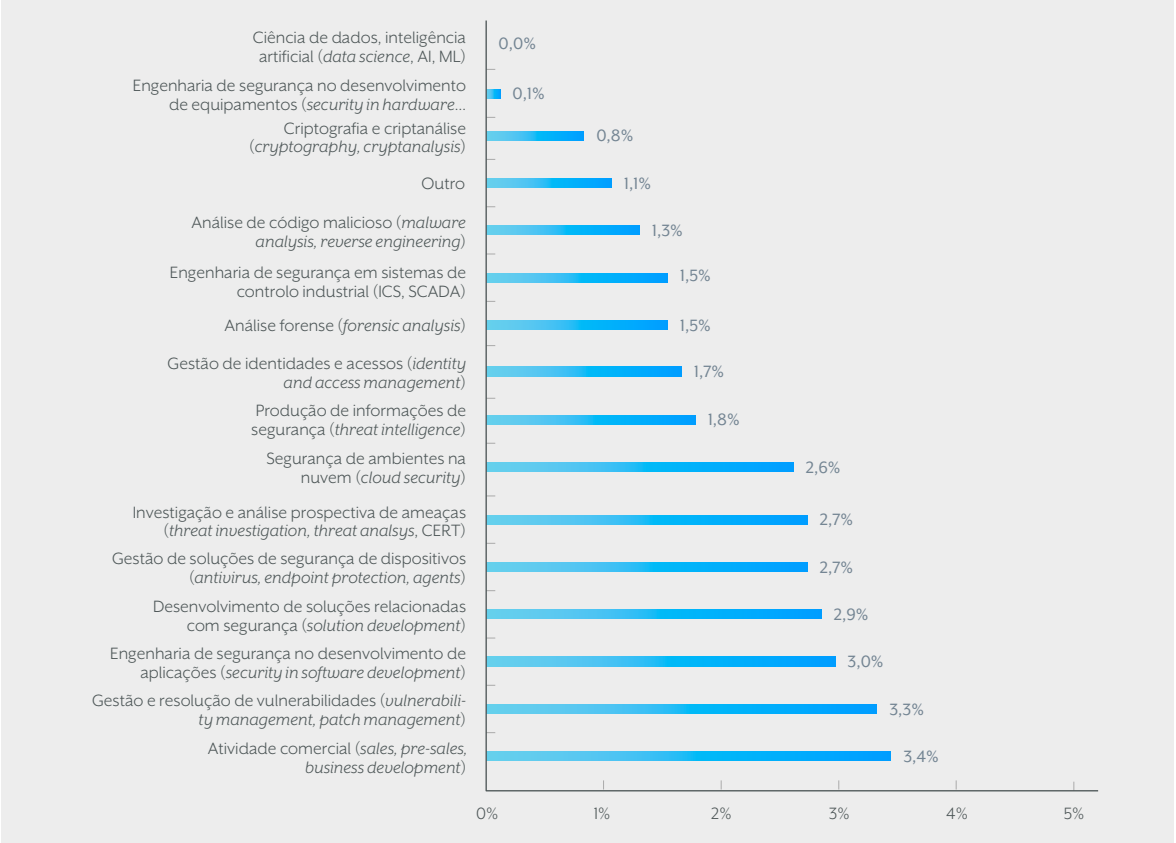
Face ao inquérito de 2019, as atividades mais relevantes continuam a ser as mesmas. No entanto a sua relevância alterou-se nos últimos dois anos: a Auditoria de segurança e a Consultoria interna ou prestação de serviços ganham importância, enquanto a Gestão de segurança da organização e a Administração de segurança em sistemas de informação a perdem.

Figura 4.12 – Principais tarefas e atividades desenvolvidas pelos profissionais de Cibersegurança



Fonte: Inquérito AP2SI aos profissionais de Cibersegurança

Figura 4.13 – Outras atividades desenvolvidas pelos profissionais de Cibersegurança

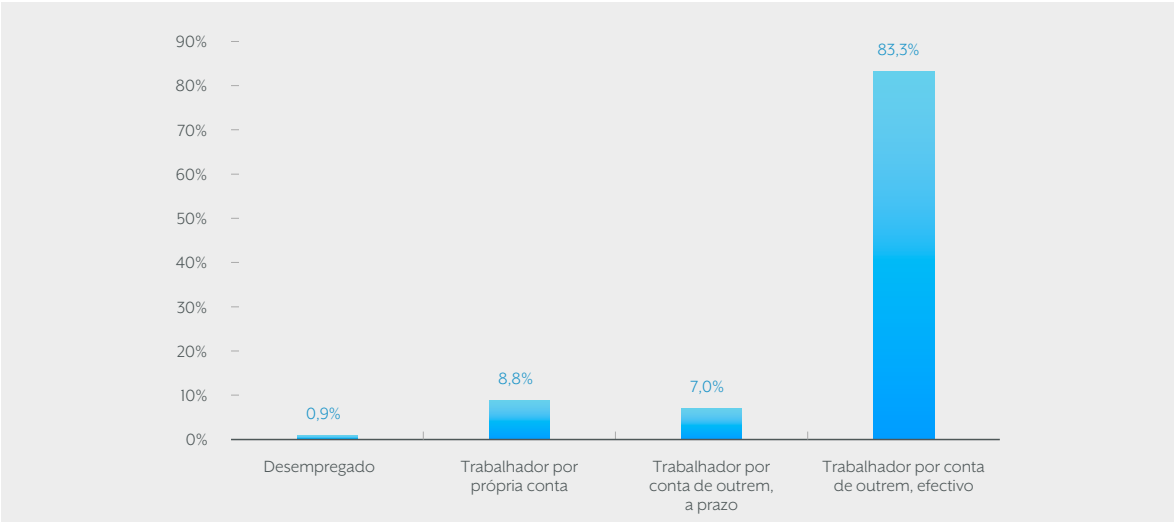


Fonte: Inquérito AP2SI aos profissionais de Cibersegurança

4.3.3 SITUAÇÃO FACE AO EMPREGO

A generalidade dos respondentes (99,1%) encontra-se empregada, estando 83,3% a trabalhar por conta de outrem com contrato sem termo ou efetivo e 7% com contrato a prazo (Figura 4.14). Apenas 8,8% dos respondentes trabalham por conta própria. O desemprego entre estes profissionais é inferior a 1%. Em relação ao inquérito de 2019, observa-se um ligeiro reforço do emprego por conta própria, uma leve redução da temporalidade (menos contratos a prazo) e uma suave redução do desemprego. Esta evolução traduz uma melhoria das condições de trabalho dos profissionais de cibersegurança.

Figura 4.14 – Situação face ao emprego dos profissionais de Cibersegurança



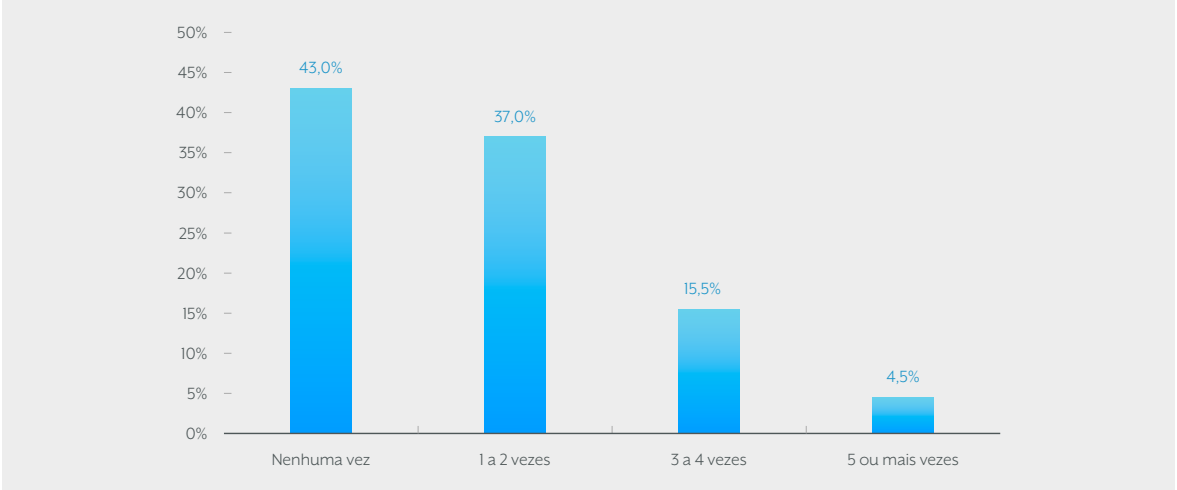
Fonte: Inquérito AP2SI aos profissionais de Cibersegurança

Quase seis em cada dez profissionais (57%) mudaram de emprego ao longo da sua vida laboral (Figura 4.15). Um em cada cinco (20%) mudou de emprego pelo menos três vezes ao longo da sua vida profissional e quase quatro em cada dez (37%) apenas uma ou duas vezes. Face aos resultados de 2019, verifica-se um aumento da proporção de profissionais que mudaram de emprego (+4 p.p.), o que é expectável com o decorrer do tempo, e um forte crescimento dos profissionais com maiores níveis de rotação, ou seja, dos que mudaram de emprego cinco ou mais vezes (+3,5 p.p.).

As transições para o desemprego são raras: apenas 10% reportaram que estiveram numa situação de desemprego ao longo da sua vida profissional, situação esta que tende a ser de duração inferior a um ano (Figura 4.16). Em relação ao inquérito de 2019, nesta dimensão a situação permanece praticamente inalterada.

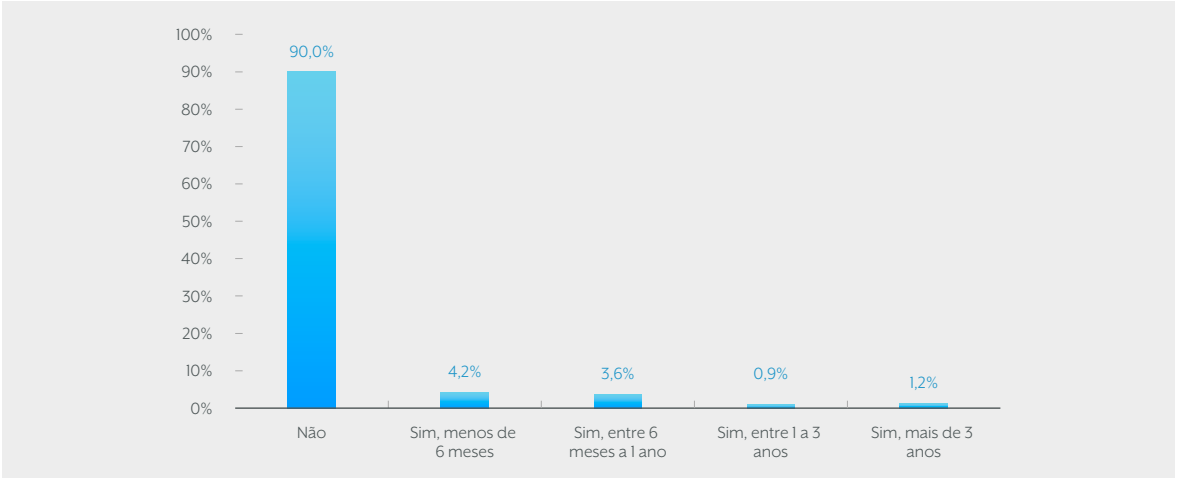
Em termos de rendimentos brutos auferidos, a maioria dos profissionais pertence aos grupos dos 20 mil aos 35 mil euros anuais (31%) e dos 35 mil aos 50 mil euros anuais (27%) (Figura 4.17). Um em cada seis (16,2%) reporta rendimentos entre 50 mil e 65 mil euros. Os grupos com menores frequências são os de mais de 65 mil euros (13,4%) e menos de 20 mil euros (12,8%). A retribuição destes profissionais é significativamente mais elevada que a de outros com níveis de qualificação similares. A retribuição média em Portugal para um quadro superior situa-se à volta dos 34 mil euros.[68] No caso dos profissionais da cibersegurança, 56,5% recebe mais de 35 mil euros anuais e 43,5% menos desse montante, portanto, a remuneração média para estes profissionais é superior à da média nacional para o mesmo nível de qualificações.

Figura 4.15 – Rotação dos profissionais de Cibersegurança – Mudanças de emprego ao longo da sua vida profissional



Fonte: Inquérito AP2SI aos profissionais de Cibersegurança

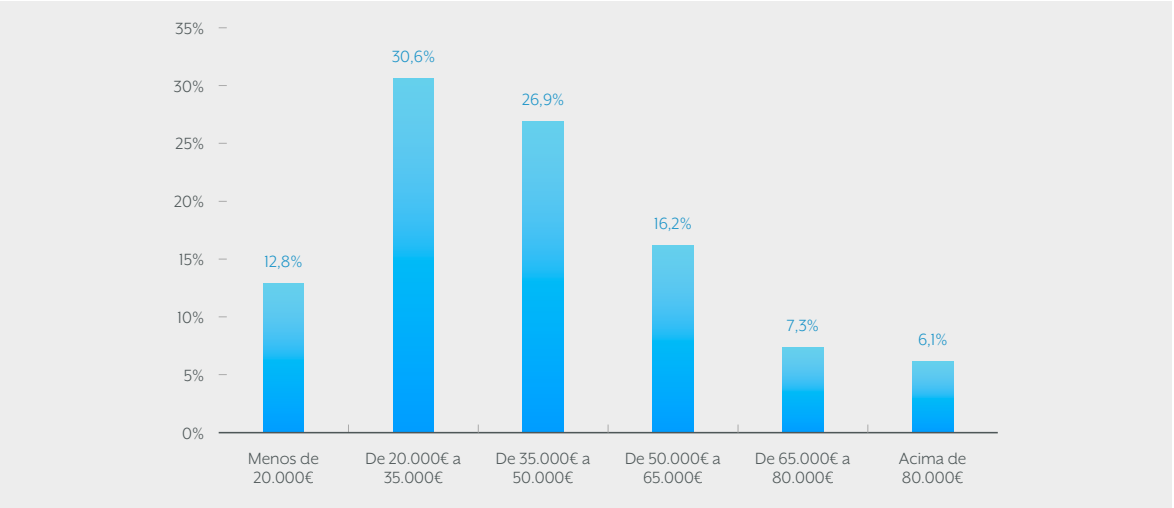
Figura 4.16 – Desemprego nos profissionais de Cibersegurança – Situações de desemprego ao longo da sua vida profissional



Fonte: Inquérito AP2SI aos profissionais de Cibersegurança

68. Valor de 2019 (INE). Ganho – Montante ilíquido mensal.

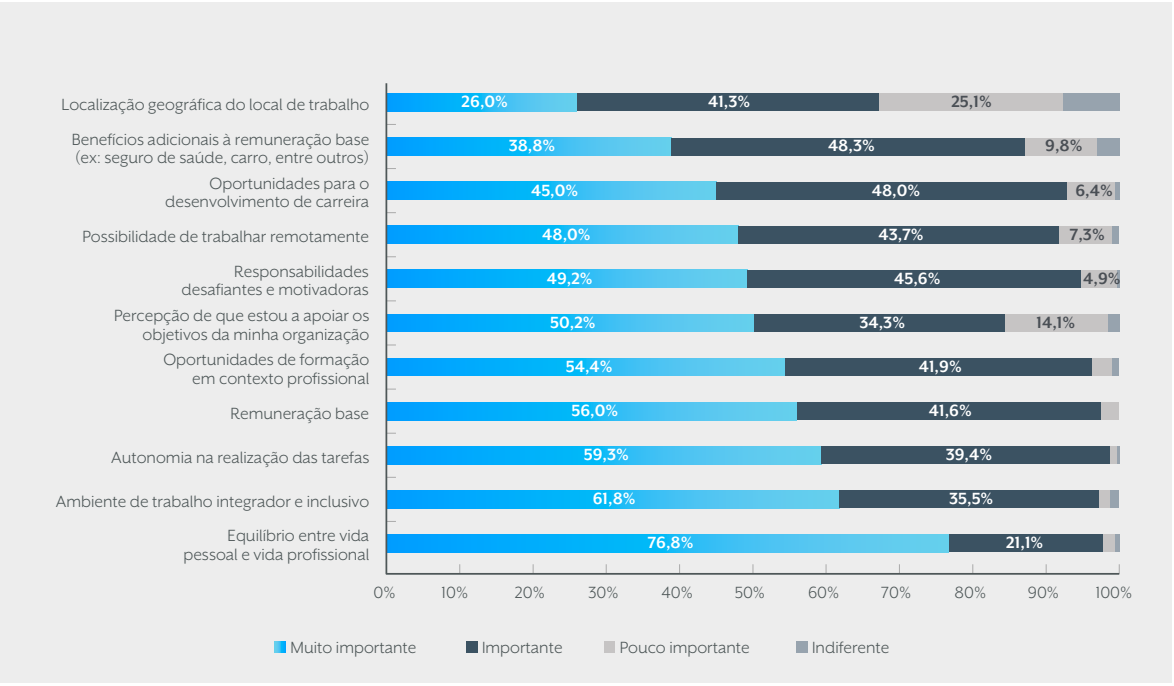
Figura 4.17 – Rendimento Bruto Anual dos profissionais de Cibersegurança



Fonte: Inquérito AP2SI aos profissionais de Cibersegurança

Face ao inquérito de 2019, observa-se uma melhoria substancial das retribuições destes profissionais. Entre os que recebem menos de 20 mil euros verificou-se uma diminuição de quase 11 p.p. A proporção de profissionais com uma remuneração entre 20 mil e 35 mil euros permaneceu praticamente inalterada. Houve um ligeiro crescimento da percentagem de profissionais que auferem entre 35 mil e 50 mil euros. Os crescimentos mais significativos foram nos grupos de retribuição mais elevados: de 50 a 65 mil euros (+5 p.p.), de 65 a 80 mil euros (+2 p.p.) e acima de 80 mil euros (+2 p.p.).

Figura 4.18 – Fatores valorizados pelos profissionais da Cibersegurança na sua atividade profissional



Fonte: Inquérito AP2SI aos profissionais de Cibersegurança

O fator mais importante para os profissionais em matéria de exercício da sua atividade laboral é o Equilíbrio entre vida pessoal e vida profissional, sendo considerado como muito importante por 76,8% dos inquiridos (Figura 4.18). Seguem-se, por ordem de importância, o Ambiente de trabalho integrador e inclusivo, a Autonomia na realização das tarefas, a Remuneração base, as Oportunidades de formação em contexto profissional e a Perceção de que os objetivos da organização estão a ser apoiados. Todos estes fatores foram indicados como muito importantes por mais de 50% dos profissionais de cibersegurança. Relativamente ao inquérito de 2019, perdem importância aspetos como as Responsabilidades desafiantes e motivadoras e as Oportunidades para o desenvolvimento de carreiras.

4.4. AS EMPRESAS DE CIBERSEGURANÇA EM PORTUGAL

Dada a inexistência de um CAE específico para as atividades de cibersegurança, para determinar, de forma aproximada, a dimensão e principais características do sector de prestação de serviços de cibersegurança é necessário recorrer a métodos indiretos. Tal como noutros âmbitos, assume-se que existem empresas que prestam este tipo de serviços de forma exclusiva, ou seja, a cibersegurança é a atividade principal e, em muitos casos, única, e que, simultaneamente, existem outras que prestam serviços de cibersegurança conjuntamente com outros serviços relacionados com as TIC.

A informação empresarial sobre as entidades do sector para fins de dimensionamento e caracterização é obtida na base de dados *ORBIS EUROPE*.[69] Esta base de dados contém informação financeira sobre empresas sedeadas na Europa, nomeadamente informação do balanço e da demonstração de resultados.

Para a identificação das empresas prestadoras de serviços de cibersegurança assumiu-se que os CAE Rev3 62 – Consultoria e Programação Informática e Atividades Relacionadas e 63 – Atividades dos Serviços de Informação são onde, à partida, se enquadram estas empresas de serviços. Para restringir o universo, realizou-se uma pesquisa textual no objeto social de cada uma das empresas associadas a esses dois CAEs, que permitiu identificar as que explicitamente referem atividades de cibersegurança no seu objeto. O conjunto de empresas identificado nesses termos é designado "grupo nuclear". As restantes empresas desses CAEs integram o denominado "grupo potencial", porque, apesar de não o indicarem explicitamente no objeto, é provável que possam prestar também serviços na área da cibersegurança.

De um total de 5.717 empresas ativas nos CAE 62 e 63,[70] 144 (2,5%) fazem parte do grupo nuclear e 5.573 (97,5%) do grupo potencial (Tabela 4.1). As empresas dos CAE de referência empregam 68.770 efetivos (1.312 no grupo nuclear e 67.458 no potencial) e têm um volume de negócios agregado de 5.575 milhões de euros (129,9 no grupo nuclear e 5.445,2 no potencial). As empresas do grupo nuclear representam 1,9% do emprego e 2,3% do volume de negócios dos CAEs de referência.

As empresas do grupo nuclear tendem a ser de menor dimensão, medida em termos de volume de negócios e de emprego, que as do grupo potencial, embora a diferença nas médias seja devida, em grande medida, à existência de grandes empresas no grupo potencial (Tabela 4.2). Trata-se, em termos médios, de empresas de reduzida dimensão, com aproximadamente um milhão de euros de faturação e em torno dos dez trabalhadores (nove nas do grupo nuclear e doze nas do grupo potencial).

Tabela 4.1 – Total de empresas, pessoal ao serviço e volume de negócios

Grupo	Total Empresas	%	Total Pessoal ao Serviço	%	Total Volume de Negócios	%
Potencial	5.573	97,5%	67.458	98,1%	5.445.211,00	97,7%
Nuclear	144	2,5%	1.312	1,9%	129.892,45	2,3%
Total	5.717	100,0%	68.770	100,0%	5.575.103,45	100,0%

Notas: Ano 2019.

Fonte: Cálculos próprios baseados em ORBIS EUROPE

Tabela 4.2 – Pessoal ao serviço e volume de negócios, por empresa

	Variável	Média	Desvio-padrão	Min	p25	p50	p75	Max
Volume de Negócios	Potencial	977,07	6.361,34	0,00	40,47	89,92	287,49	166.101,00
	Nuclear	902,03	3.248,37	0,10	37,59	106,32	381,40	8.194,86
Pessoal ao serviço	Potencial	12,10	71,46	1,00	1,00	2,00	5,00	2.285,00
	Nuclear	9,11	24,65	1,00	1,00	2,00	6,50	230,00

Notas: Ano 2019.

Fonte: Cálculos próprios baseados em ORBIS EUROPE

69. Produzida pela empresa Bureau van Dijk.

70. Todos os dados são de 2019.

O ativo total também reflete a diferença de dimensão entre ambos os grupos, embora a diferença nas médias seja pouco expressiva (Tabela 4.3). A grande diferença neste âmbito é que as empresas do grupo nuclear tendem a financiar o ativo recorrendo, em maior medida, a capitais alheios (e, em menor medida, a capitais próprios) que as do grupo potencial.

Em termos médios, não existem diferenças significativas em termos de rentabilidade operacional (*Cash-flow*, Valor Acrescentado e EBITDA) entre as empresas do grupo nuclear e do grupo potencial (Tabela 4.4).[71] Tal como noutros agregados, a rentabilidade máxima no grupo potencial é muito superior à do grupo nuclear, devido essencialmente às diferenças em termos de dimensão empresarial.

Tabela 4.3 – Ativo total, capitais próprios e passivo total, por empresa

	Variável	Média	Desvio-padrão	Min	p25	p50	p75	Max
Ativo Total	Potencial	889,52	5.921,86	0,01	25,11	77,40	274,26	191.888,00
	Nuclear	879,27	3.490,20	0,08	25,83	81,92	339,34	34.912,20
Capitais Próprios	Potencial	331,32	2.651,54	-18 113,91	3,91	26,42	103,95	100.967,50
	Nuclear	174,94	589,56	-1 723,81	4,07	22,72	94,66	4 695,02
Passivo Total	Potencial	557,95	3.865,79	-7,05	12,15	40,21	155,98	120.309,50
	Nuclear	704,33	3.137,11	0,75	11,65	50,30	226,71	31.814,08

Notas: Ano 2019.

Fonte: Cálculos próprios baseados em ORBIS EUROPE

Tabela 4.4 – *Cash-flow*, valor acrescentado e ebitda, por empresa

	Variável	Média	Desvio-padrão	Min	p25	p50	p75	Max
Cash-Flow	Potencial	100,89	1.147,11	-11.890,82	0,41	7,38	28,13	40.983,92
	Núcleo	100,67	657,92	-421,20	-1,40	9,50	29,93	7.391,40
Valor Acrescentado	Potencial	522,79	3.556,06	-11.827,14	18,64	48,15	143,24	113.073,00
	Núcleo	407,03	1.459,25	-58,12	16,55	58,13	160,03	15.371,03
EBITDA	Potencial	119,51	1.290,12	-15.854,12	0,98	9,56	34,92	47.355,73
	Núcleo	115,18	690,34	-384,66	-1,08	10,77	41,12	7 665,98

Notas: Ano 2019.

Fonte: Cálculos próprios baseados em ORBIS EUROPE

Em síntese, o sector da cibersegurança em Portugal, constituído por empresas cujo volume de negócios procede em grande medida desta atividade, integra 144 empresas, que empregam aproximadamente 1.300 trabalhadores e faturam cerca de 130 milhões de euros.

Esta definição restrita do sector, que delimita um grupo nuclear relativamente pequeno, pode não refletir a abrangência real do sector. Outras empresas que desenvolvem as suas operações no âmbito das TIC (CAEs 62 e 63) também poderão estar a vender produtos ou a prestar serviços de cibersegurança, ainda que essas atividades não constem no seu objeto social de forma explícita. Desta forma, potencialmente pode integrar o sector da cibersegurança um universo de empresas ligadas à área das TIC, cuja consideração para efeitos de dimensionamento elevaria significativamente a dimensão sectorial. Assim sendo, o número de empresas, o número de trabalhadores e o volume de negócios do grupo potencial devem ser interpretados, conjuntamente com os do grupo nuclear, como tetos do sector da cibersegurança em Portugal, quando aplicada uma definição sectorial extremamente abrangente.[72]

71. No entanto, os indicadores refletem uma maior rentabilidade das empresas pertencentes ao grupo nuclear que se situam entre a mediana e o percentil 75%.

72. Note-se que é um limite máximo inatingível, dado que as empresas do grupo potencial desenvolvem primordialmente, de acordo como o seu objeto social, outras atividades vinculadas com as TIC, para além da cibersegurança – sendo que, provavelmente, na maioria dos casos nem sequer exercem qualquer atividade relacionada com a cibersegurança.


BITCOIN · DIGITAL · DECENTRALIZED · PEER TO PEER
STANDARD METALS
1 OZ .999 FINE COPPER

DESTAQUES CAPÍTULO IV

O aumento da procura de profissionais e de serviços de cibersegurança, por parte das empresas, tem de ser acompanhado de uma oferta de recursos humanos especializados e de empresas de prestação de serviços de cibersegurança.

Entre 2013 e 2019, o número de diplomados em TIC em Portugal cresceu cerca de 75%, um valor muito acima do crescimento do número de diplomados em todas as áreas, que não alcançou os 3%. No mesmo período, o crescimento de diplomadas em TIC foi de cerca de 33%, portanto, inferior ao crescimento médio na área.

A percentagem de diplomados em TIC em Portugal é das mais baixas da União Europeia (2,3%), situando-se 1,5 p.p. abaixo da média comunitária (3,8%). A percentagem de diplomadas em TIC no país (0,4%) é metade da média da União (0,8%), sendo igualmente das mais baixas a nível europeu (UE-28).

Em 2020, o número total de especialistas em TIC empregados em Portugal ultrapassava os 190 mil. Entre 2015 e 2020, a oferta de especialistas em TIC no país aumentou em mais de 57 mil trabalhadores. Este crescimento permitiu reforçar o peso dos especialistas nesta área no emprego total (de 3% a 4%) e aproximar-se da média da União Europeia (4,3%). Nos últimos cinco anos, observa-se um ligeiro envelhecimento desses profissionais, em linha com o que acontece noutros países da Europa.

Quase cinco em cada dez (47,0%) profissionais de cibersegurança em Portugal têm 40 anos ou menos e quase quatro em cada dez (39,7%) têm entre 41 e 50 anos. A maioria dos profissionais é do sexo masculino (84,2%), não obstante, nos últimos anos tem havido um aumento da participação feminina no sector. Quase dois terços dos profissionais (62,7%) têm até dez anos de experiência e mais de um quarto (27,6%) entre onze e vinte anos de experiência.

A maioria dos profissionais de cibersegurança (83%) possui estudos superiores: 4,2% possuem doutoramento, 52,1% uma licenciatura pré-Bolonha ou um mestrado e 26,7% uma licenciatura de Bolonha ou um bacharelato. Nos últimos anos, tem-se verificado um reforço da qualificação média dos profissionais do sector.

Na região de Lisboa e Vale do Tejo (LVT) localizam-se seis em cada dez profissionais de cibersegurança (58,2%) e nas regiões Norte e Centro à volta de um terço dos mesmos (35,8%). A área metropolitana de Lisboa continua a ser um polo de atração para os profissionais do sector.

Cinco em cada dez profissionais (50,0%) desenvolve a sua atividade no sector dos Serviços e produtos de telecomunicações e tecnologias de informação e quase um em cada dez (11,5%) na Administração Pública e Estado. Outros sectores relevantes em termos de emprego para estes profissionais são a Indústria, o Ensino, academia, investigação e desenvolvimento e as Instituições bancárias, financeiras e seguros.

As principais atividades desenvolvidas pelos profissionais de cibersegurança são a Auditoria de segurança (10,6%), a Consultoria interna ou prestação de serviços (10,2%), a Gestão de segurança da organização (8,6%) e a Administração de segurança em sistemas de informação (6,1%). Nos últimos anos, as atividades desempenhadas por estes profissionais continuam a ser genericamente as mesmas.

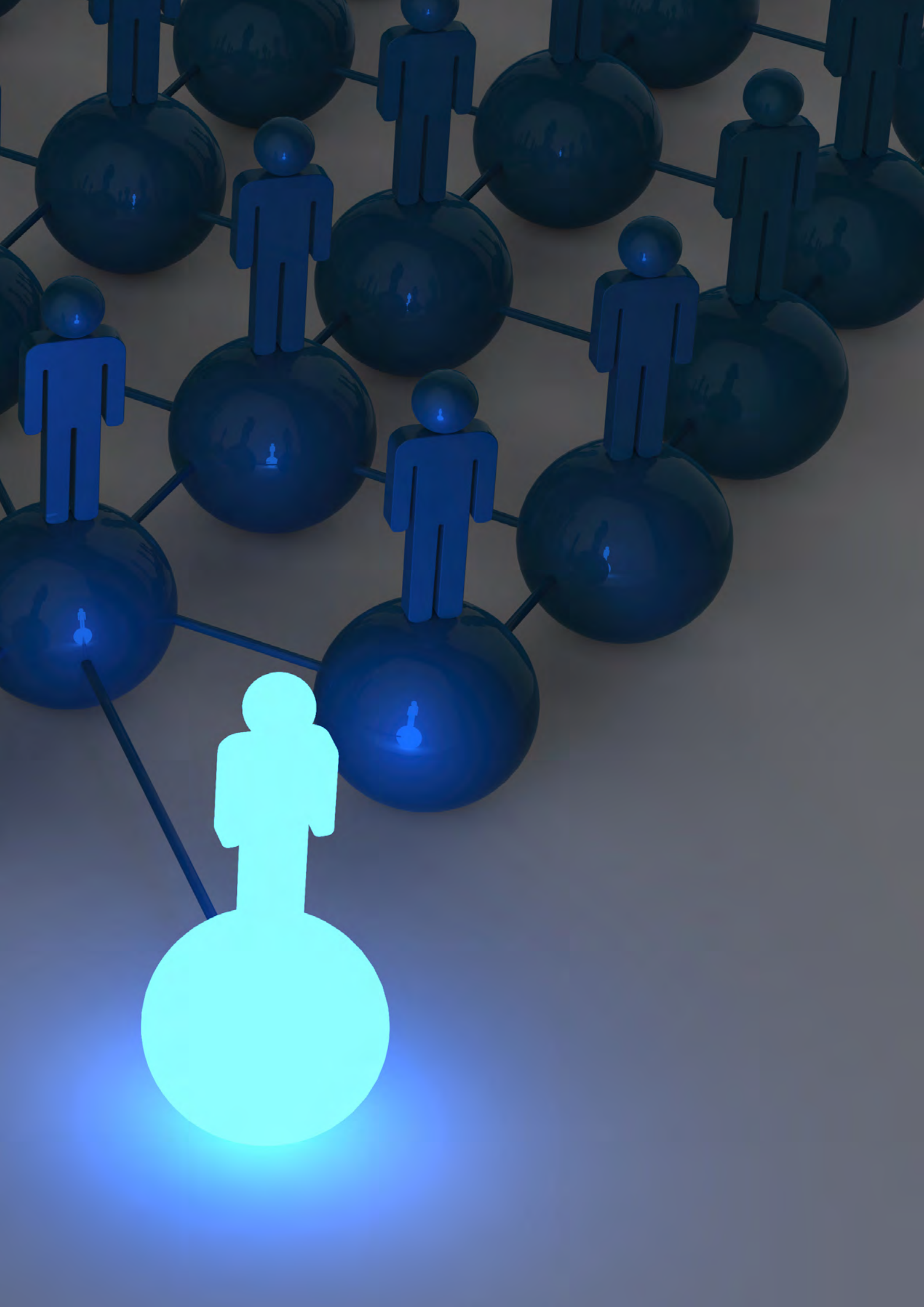
O desemprego neste sector tem caráter friccional (resulta de mudanças de emprego), sendo inferior a 1%. Dos empregados, apenas trabalham por conta própria 9% do total. Os restantes trabalham por conta de outrem, maioritariamente com contratos sem termo ou efetivos. Nos últimos anos, verificou-se um reforço do autoemprego, uma ligeira redução da temporalidade e uma pequena diminuição do desemprego.

Quase seis em cada dez profissionais aufere um rendimento entre 20 mil e 50 mil euros anuais (31% entre 20 mil e 35 mil euros e 27% entre 35 mil e 50 mil euros). Quase três em cada dez recebe mais de 50 mil euros. Os restantes 13%, aproximadamente, têm salários inferiores a 20 mil euros. Nos últimos anos, houve uma melhoria das remunerações dos profissionais de cibersegurança. A remuneração média no sector é superior à da média nacional para o mesmo nível de qualificações.

Considerando apenas empresas cujo volume de negócios procede, em grande medida, da prestação de serviços de cibersegurança, o sector da cibersegurança em Portugal é constituído por 144 empresas, que empregam aproximadamente 1.300 trabalhadores e têm um volume de negócios conjunto de cerca de 130 milhões de euros.

Não obstante, uma definição tão restrita de empresas de cibersegurança poderá estar a subestimar a dimensão real do sector, dado que um número crescente de empresas do setor das TIC está a prestar serviços de cibersegurança, gerando a partir desta atividade uma parte substantiva do seu volume de negócios.

CAPÍTULO V
A PROCURA DE CIBERSEGURANÇA NAS PMES PORTUGUESAS



CAPÍTULO V
A PROCURA DE CIBERSEGURANÇA NAS PMES PORTUGUESAS

5.1 ENQUADRAMENTO

Na última década, as PMEs portuguesas têm vindo a aumentar a sua exposição digital, o volume de dados que administram e, em geral, os seus níveis de digitalização. As principais alavancas do reforço da componente digital das PMEs são as novas formas de divulgação e notabilização *online*, a explosão do *e-commerce*, a crescente inter-relação com *stakeholders* através de redes informáticas, a utilização de *software*, sistemas e dispositivos em modo remoto e a intensificação da digitalização e a emergência de novas tecnologias disruptivas conectadas à Internet. Genericamente as PMEs portuguesas estão digitalmente menos expostas, integradas e desenvolvidas que as suas congéneres europeias, mas com os atuais níveis de conexão e digitalização já enfrentam riscos significativos em matéria de cibersegurança.

A finalidade última deste capítulo é apresentar os resultados de um inquérito sobre a situação da cibersegurança nas PMEs portuguesas e sobre as suas principais práticas neste domínio. No inquérito, promovido pelo Centro Nacional de Cibersegurança e com o apoio do IAPMEI, participaram 641 PMEs portuguesas, representativas da maioria dos setores da economia do país. O objetivo do inquérito é duplo. Por um lado, tenciona-se balizar os níveis de exposição digital das PMEs portuguesas e identificar as tipologias de dados que gerem, assim como os potenciais impactos dos incidentes nesse domínio. Por outro, pretende-se conhecer as práticas, protocolos e medidas de cibersegurança nas PMEs portuguesas, tentando explorar e analisar diferenças em função da dimensão empresarial e do setor de atividade em que operam. Todos os dados dizem respeito ao ano de 2022.

A caracterização das empresas participantes no inquérito, assim como os seus níveis de exposição digital e de negócio *online* são sistematizados na Box I. Na secção 3.2 apresentam-se as diferentes tipologias de dados geridos pelas PMEs portuguesas, bem como os principais impactos derivados de incidentes de segurança das TIC. A secção 3.3 é dedicada integralmente à cibersegurança. Inicialmente analisam-se a organização das funções de cibersegurança e os recursos financeiros e humanos a ela dedicados. Discutem-se também a problemática da contratação/retenção de profissionais, as fontes de recrutamento e as políticas de formação dos trabalhadores. As principais medidas de cibersegurança utilizadas pelas PMEs, assim como as principais barreiras à sua implementação efetiva são apresentadas a seguir. Incluem-se ainda resultados sobre a frequência, a tipologia e os custos dos ciberataques e sobre a cultura de cibersegurança nas PMEs portuguesas.

Box I – Respondentes e exposição digital

No inquérito participaram 641 empresas. A amostra cobre a totalidade do território nacional, tendo respondido empresas das cinco NUT II do Continente, bem como dos territórios insulares. Das empresas participantes, 36,4% têm a sua sede social no Norte, 28,5% no Centro e 24,9% em Lisboa e Vale do Tejo (LVT). As empresas do Algarve representam 4,1% da amostra, as do Alentejo 3,5% e as das Ilhas (Açores e Madeira) 2,5%.

As empresas da indústria têm um peso de 31,9% e as da construção de 12,9%. O sector serviços representa mais de 55% da amostra. Concretamente, 31,2% das empresas pertencem aos sectores do comércio, da restauração e do alojamento, 11,0% a sectores de serviços de reduzido valor acrescentado (v.a.) e 12,9% a sectores de serviços de elevado valor acrescentado (v.a.)

Quase 90% das empresas participantes são PMEs. As grandes empresas representam apenas 2,0% do total e as microempresas 9,2%. Dois terços das respondentes (66,8%) são pequenas empresas (10 a 49 trabalhadores) e pouco mais de um quinto (22,0%) médias empresas (50 a 250 trabalhadores).

Quase quatro em cada dez empresas participantes (38,2%) faturam entre 300.000 e dois milhões de euros e três em cada dez (29,0%) entre dois e cinco milhões de euros. Aproximadamente um quarto das empresas (26,3%) tem um volume de negócios superior a cinco milhões de euros. Desse grupo, à volta de 40% ultrapassa os dez milhões de euros. Apenas 6,4% das empresas fatura menos de 300.000 euros.

Quase dois terços das empresas participantes (65,8%) são sociedades de responsabilidade limitada e quase um quarto são sociedades anónimas (23,7%). Entre as empresas pequenas, três quartos (74,3%) são sociedades de responsabilidade limitada e um sexto (16,6%) sociedades anónimas. Esta tipologia societária é a forma jurídica dominante entre as médias empresas, dado que uma em cada duas é uma sociedade anónima (49,6%).

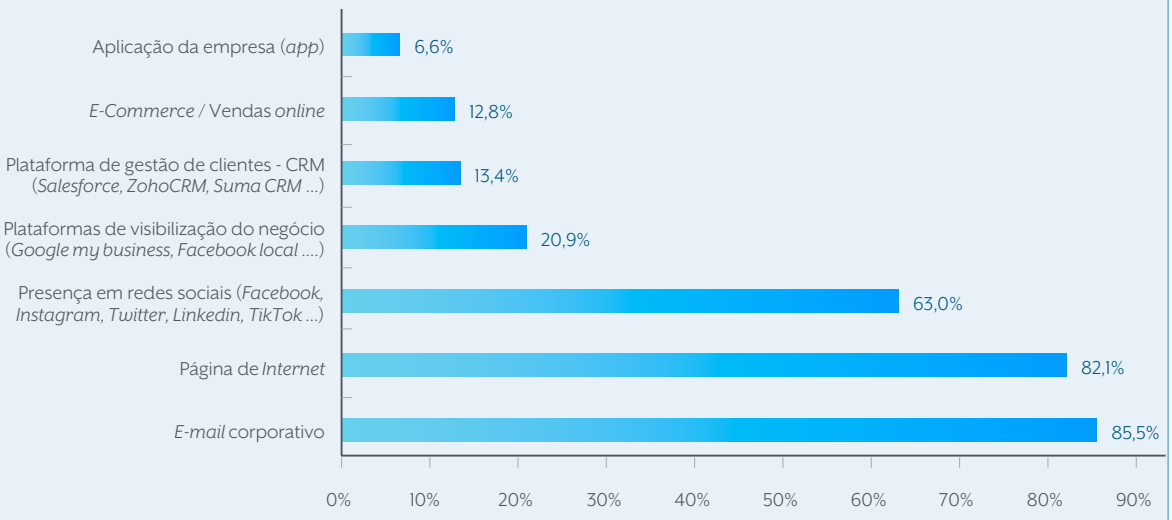
Dadas as implicações em termos de cibersegurança da crescente exposição *online* das PMEs portuguesas é fundamental caracterizar a sua atividade e presença digital. Em mais de um terço das empresas participantes (37,4%), as vendas *online* são inferiores a 20% do volume de negócios. Para 5,8% das empresas são superiores a 20% – para 3% das empresas representam entre 20 e 40% e apenas para 2,8% mais de 40%. Quase 57% não sabe (ou não responde) qual o peso das vendas através de canais digitais no seu volume de negócios.

Quase todas as empresas inquiridas têm presença digital, embora a intensidade e as formas de participação no universo digital difiram significativamente entre organizações (Figura B-I.1). 85,5% das empresas possuem *e-mail* corporativo e 82,1% página de Internet, não obstante, apenas 6,6% das empresas têm uma *app* corporativa. Quase duas em cada três empresas (63,0%) está presente nas redes sociais e uma em cada cinco (20,9%) em plataformas de visibilização de negócios. Um número reduzido de empresas (13,4%) dispõe de alguma plataforma de gestão de clientes. Apenas 12,8% das empresas participantes realizam vendas *online* .

As principais diferenças entre pequenas e médias empresas é que mais médias empresas possuem página de Internet (90,8% versus 82,9%) e aplicações de empresa (12,1% versus 3,5%) (Figura B-I.2 e Figura B-I.3). Também se observam diferenças consideráveis no que se refere à presença nas redes sociais (76,6% nas médias versus 60,0% nas pequenas) e às vendas *online* (15,6% nas médias versus 12,1% nas pequenas).

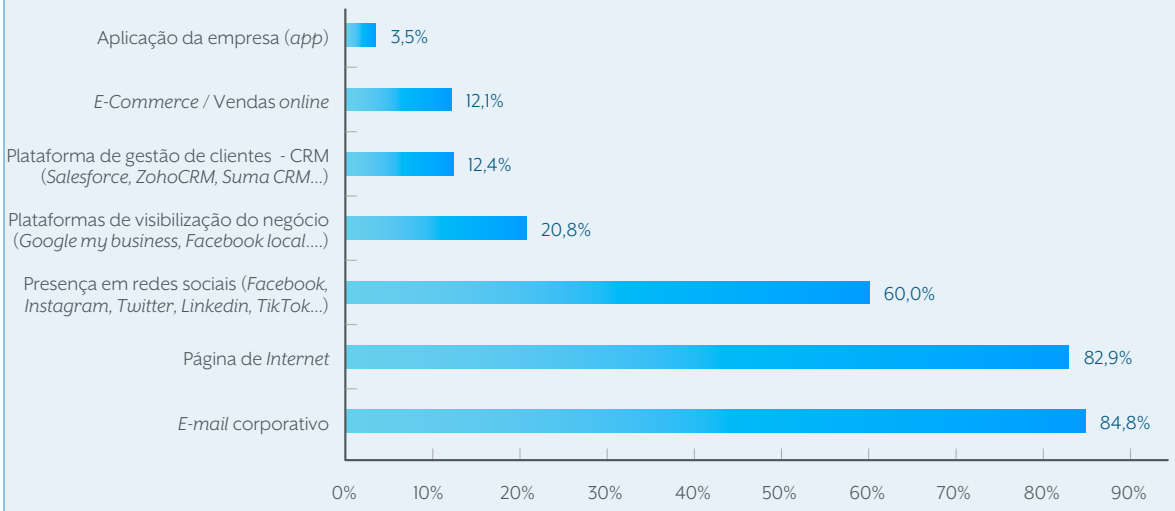
Box I – Continuação

Figura B-I.1 – Formas de presença digital, para todas as empresas, Portugal, % de empresas



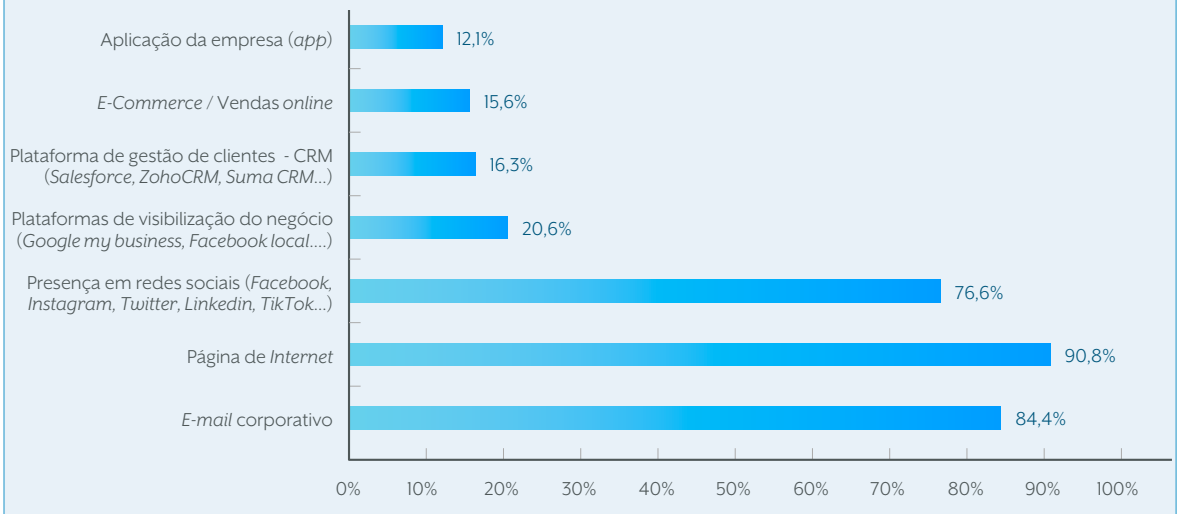
Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Figura B-I.2 - Formas de presença digital das pequenas empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Figura B-I.3 - Formas de presença digital das médias empresas, Portugal, % de empresas

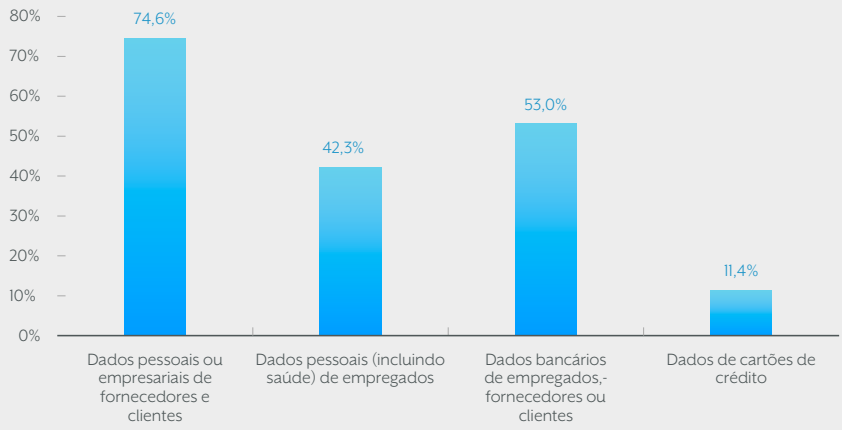


Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

5.2 DADOS GERIDOS E IMPACTOS DE INCIDENTES

As PMEs portuguesas processam diferentes tipos de informação digital. Cerca de três em cada quatro empresas (74,6%) processam informação pessoal ou empresarial de fornecedores e clientes e algo mais de metade (53,0%) dados bancários de empregados, fornecedores e clientes (Figura 5.1). Mais de quatro em cada dez (42,3%) gerem informação pessoal dos seus empregados e quase uma em cada nove (11,4%) dados de cartões de crédito.

Figura 5.1 – Tipo de informação digital processada, para todas as empresas, Portugal, % de empresas

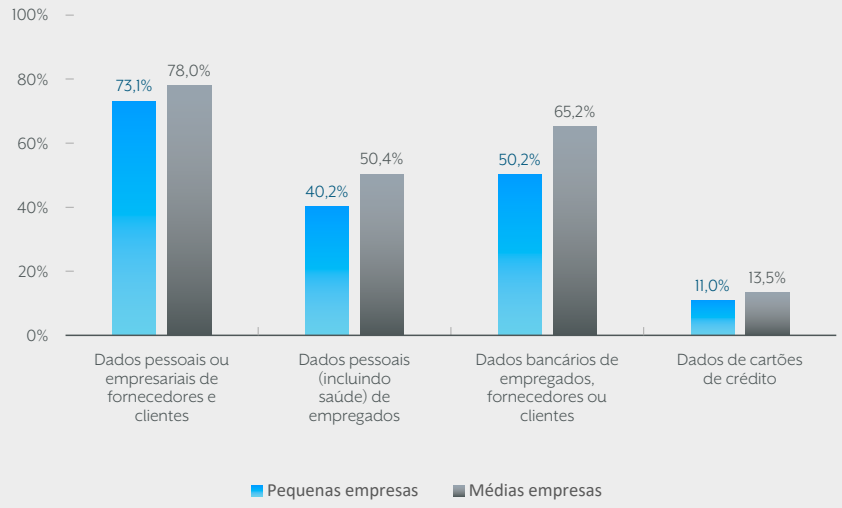


Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

As grandes diferenças por dimensão empresarial nesta matéria são a maior percentagem de empresas médias que processam dados pessoais dos seus empregados (50,4% nas médias versus 40,2% nas pequenas) e dados bancários de empregados, fornecedores ou clientes (65,2% nas médias versus 50,2% nas pequenas) (Figura 5.2). Relativamente ao tratamento de dados de fornecedores e clientes e de cartões de crédito, as diferenças por dimensão empresarial são relativamente reduzidas.

As empresas de construção são as que processam menos informação digital. São as menos dinâmicas em todas as dimensões, exceto no processamento de informação bancária de empregados, fornecedores e clientes, onde as empresas dos sectores de comércio e afins e de serviços de reduzido valor acrescentado (v.a.)[73] apresentam percentagens mais baixas Contrariamente, as empresas que processam mais informação digital são as de serviços de elevado valor acrescentado (v.a.). Estas empresas lideram em todas as dimensões, exceto no processamento de informação de caráter pessoal dos empregados, onde as mais ativas são as do sector industrial.

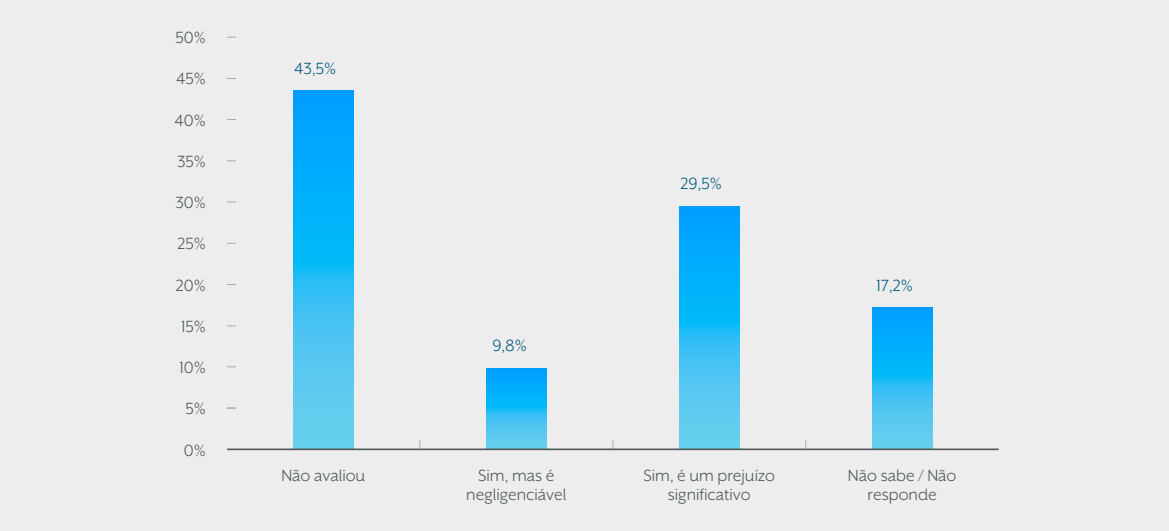
Figura 5.2 – Tipo de informação digital processada, por dimensão empresarial, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

73. O valor acrescentado corresponde à diferença entre o valor dos bens produzidos e os custos dos bens intermédios utilizados na sua produção.

Figura 5.3– Avaliação do impacto financeiro na organização de uma possível interrupção da rede ou das TIC, para todas as empresas, Portugal, % de empresas.



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Relativamente ao impacto financeiro de eventuais interrupções da rede ou das TIC, 39,3% das empresas inquiridas avaliou esses impactos, 43,5% não o fez e as restantes não sabem (ou não respondem) (Figura 5.3). Das que avaliaram esse impacto financeiro, uma em cada quatro consideram que implicaria perdas negligenciáveis, enquanto que para três em cada quatro resultaria em prejuízos significativos.

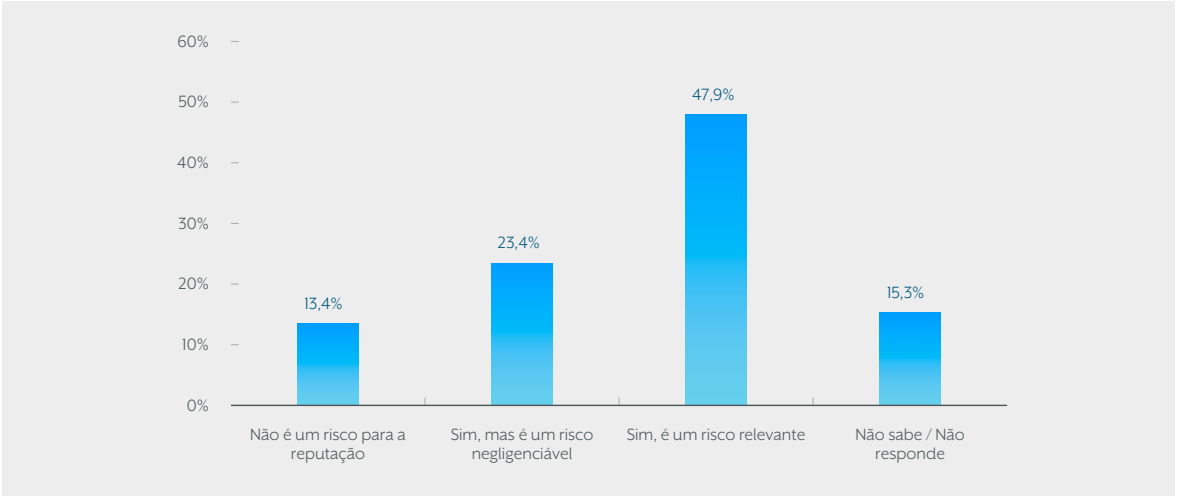
Na análise por dimensão, a principal diferença é que, curiosamente, a proporção de empresas médias que não avaliam estes impactos é maior que a de pequenas empresas (44,7% versus 41,8%). A percentagem das que não sabem (ou não respondem) entre as empresas médias é bastante inferior (12,1% versus 18,5%). Entre as empresas que avaliam os impactos, a percentagem das que consideram que o impacto pode ser significativo é cinco pontos percentuais mais elevado nas médias que nas pequenas empresas (34,8% versus 29,4%).

Os sectores onde uma maior proporção de empresas não avalia esses riscos são os de serviços de reduzido v.a., a indústria e a construção. O sector onde uma maior percentagem de empresas considera que o impacto é pouco significativo é o da construção. Este sector apresenta a menor percentagem de empresas que julgam que o impacto é significativo (19,8%) e a maior percentagem das que entende que não é significativo (12,3%). Contrariamente, as empresas de serviços de elevado v.a. são as que atribuem grande importância a estes riscos. Este sector apresenta a maior percentagem de empresas que consideram que o impacto é significativo (40,7%) e das menores percentagens entre as que consideram que não é significativo (8,6%) – juntamente com a indústria.

Em relação aos riscos reputacionais no caso de ocorrer uma violação de dados, quase metade das empresas inquiridas (47,9%) considera que é um risco relevante e quase um quarto (23,4%) que é um risco pouco expressivo (Figura 5.4). Para 13,4% das empresas respondentes estes incidentes não constituem um risco para a empresa. Neste caso, 15,3% das empresas não sabe (ou não responde) se a violação de dados é ou não um risco com impactos sobre a sua reputação.

À medida que aumenta o seu tamanho, mais empresas associam riscos reputacionais a este tipo de incidentes (75,2% nas médias empresas versus 69,4% nas pequenas empresas). Adicionalmente, nas empresas de maior tamanho, neste caso as médias, uma maior percentagem considera que os riscos na reputação das violações de informação podem ser relevantes e, consequentemente, ter impactos significativos sobre a organização (51,1% nas médias empresas versus 45,3% nas pequenas empresas).

Figura 5.4 – Avaliação dos danos na reputação da organização no caso de ocorrer uma violação de dados, para todas as empresas, Portugal, % de empresa



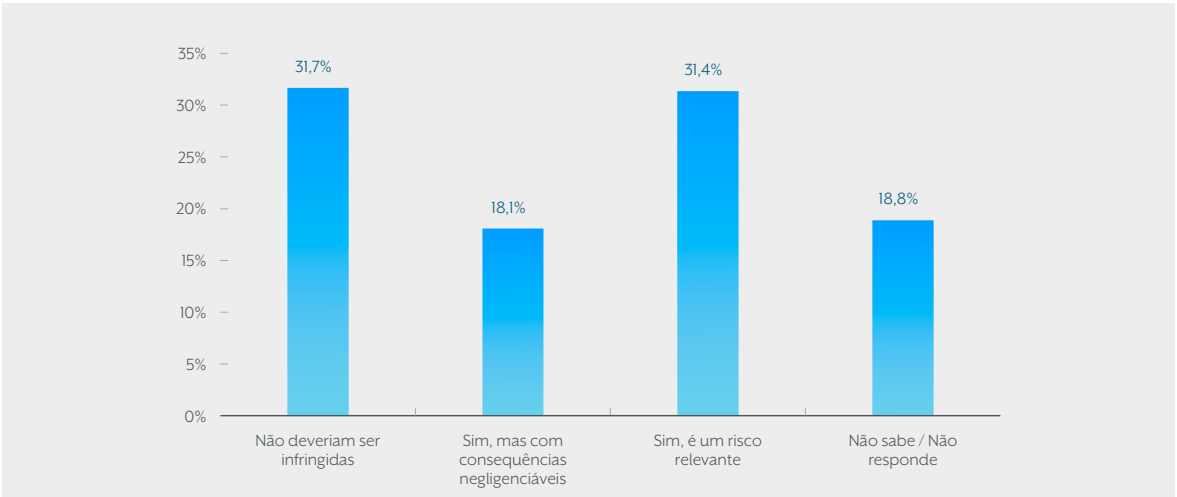
Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

O sector onde é percecionado um maior risco reputacional é o dos serviços de elevado v.a. (92,6% das empresas, sendo que 71,6% considera que é um risco relevante) – só 4,9% não sabe ou não responde. Nos sectores da construção e do comércio e afins é onde uma maior proporção de empresas considera que estes incidentes não são um risco para a sua reputação (16,0% e 15,9%, respetivamente) – contra 2,5% no caso das empresas do sector de serviços de elevado v.a.

Em relação à possibilidade de as organizações não cumprirem obrigações contratuais para com terceiros no caso de ocorrer uma violação de dados ou uma interrupção da rede, metade das empresas (49,5%) consideram que existe risco de incumprimento (Figura 5.5). Delas, quase dois terços entendem que o risco é relevante (31,4% do total), enquanto que para pouco mais de um terço (18,1%) o risco tem pouca importância. Quase uma em cada cinco empresas (18,9%) não sabe (ou não responde) se o risco de incumprimento de contratos com terceiros, em resultado da violação de dados ou da interrupção da rede, é uma possibilidade efetiva ou não.

Existem divergências na perceção deste risco entre empresas de diferente dimensão. A percentagem de pequenas empresas que considera pouco prováveis os incumprimentos contratuais derivados da violação de dados ou da interrupção da rede é superior à das médias empresas com a mesma opinião (34,6% nas pequenas empresas versus 25,5% nas médias empresas).

Figura 5.5 – Obrigações contratuais da empresa para com terceiros no caso de violação de dados ou interrupção da rede, para todas as empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

O risco de não cumprimento existe para 57,5% das médias e 45,1% das pequenas empresas. Adicionalmente, para uma maior proporção de médias empresas essa eventual falta de cumprimento dos contratos é relevante (35,5% nas médias empresas versus 28% nas pequenas empresas).

Existem também divergências por sectores. As empresas industriais são as que consideram menos provável o incumprimento dos contratos por violação de dados ou interrupção da rede, enquanto que as de serviços de elevado v.a. são as que atribuem maior probabilidade a esse incumprimento. Sete em cada dez destas empresas (70,4%) de serviços consideram que estes incidentes podem provocar um incumprimento com consequências. Entre estas empresas, três em cada dez considera que é um risco negligenciável e sete em cada dez que é um risco relevante.

5.3 FUNÇÕES DE CIBERSEGURANÇA

Os riscos derivados do aumento da exposição digital, da posse e gestão de dados privados e da digitalização em geral tem levado as PMEs portuguesas a reforçar os seus níveis de cibersegurança. Na última década estas empresas aumentaram os recursos alocados a cibersegurança e reorganizaram-se funcionalmente, melhoraram as suas práticas, protocolos e medidas de segurança TIC, reforçaram a sua cultura de cibersegurança e fortaleceram a sua capacidade de proteção e resposta a ciberataques.

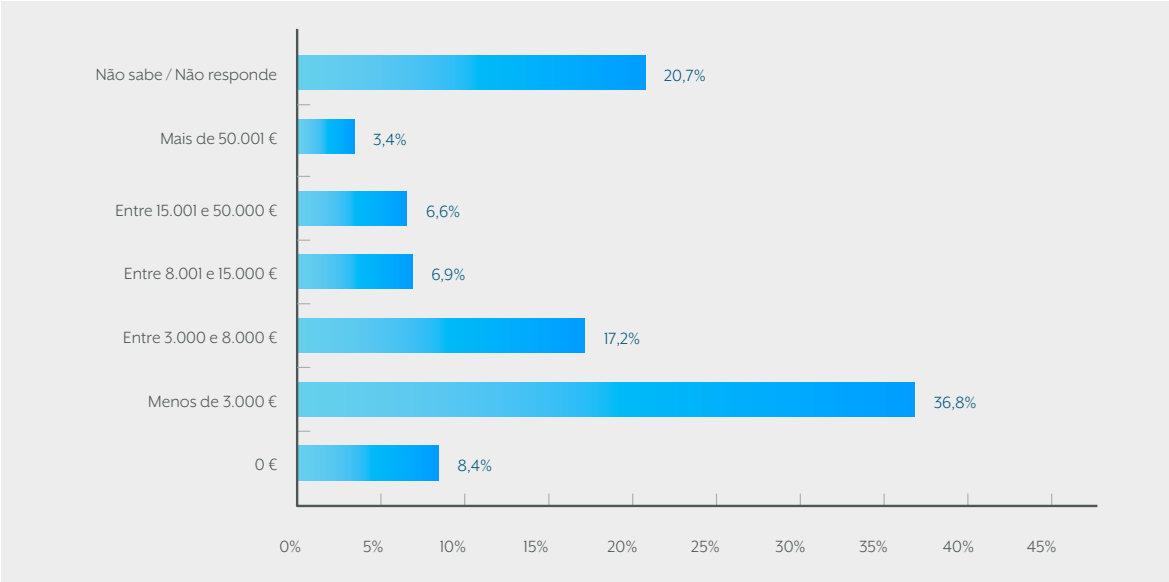
O orçamento anual para as funções de cibersegurança nas PMEs portuguesas difere significativamente. Mais de um terço das empresas (36,8%) dedica menos de 3.000 euros por ano a estas funções, enquanto que aproximadamente um outro terço (34,1%) destina um valor superior (Figura 5.6). Metade das que afetam mais de 3.000 euros, alocam entre 3.000 e 8.000 euros. Quase 7% destinam à cibersegurança entre 8.000 e 15.000 euros, 6,6% entre 15.000 e 50.000 euros e 3,4% mais de 50.000 euros. Entre as que dedicam mais de 50.000 euros, quase 1% tem um orçamento anual de mais de 300.000 euros. Uma em cada cinco empresas (20,7%) não sabe (não responde) quanto despende anualmente em segurança informática e quase uma em cada dez (8,6%) não tem orçamento para este fim.

Mais de 40% das pequenas empresas (41,6%) dedicam menos de 3.000 euros anuais às funções de cibersegurança, enquanto que apenas 24,8% das empresas médias possuem orçamentos inferiores a esse limiar (Figura 5.7 e Figura 5.8). Em 7,2% das pequenas empresas e em 4,3% das médias não existe qualquer orçamento para funções de cibersegurança.

Mais de metade das empresas médias (53,9%) têm um orçamento de cibersegurança superior a 3.000 euros; 18,4% entre 3.000 e 8.000 euros; 12,8% entre 8.000 e 15.000 euros; e, 14,9% entre 15.000 e 50.000. Só 7,8% das empresas médias dedicam mais de 50.000 euros à cibersegurança. No caso das pequenas empresas, o investimento anual em cibersegurança é superior a 3.000 euros em menos de 30% das empresas (29,8%). O orçamento em cibersegurança só é superior a 50.000 euros em uma em cada cem empresas.

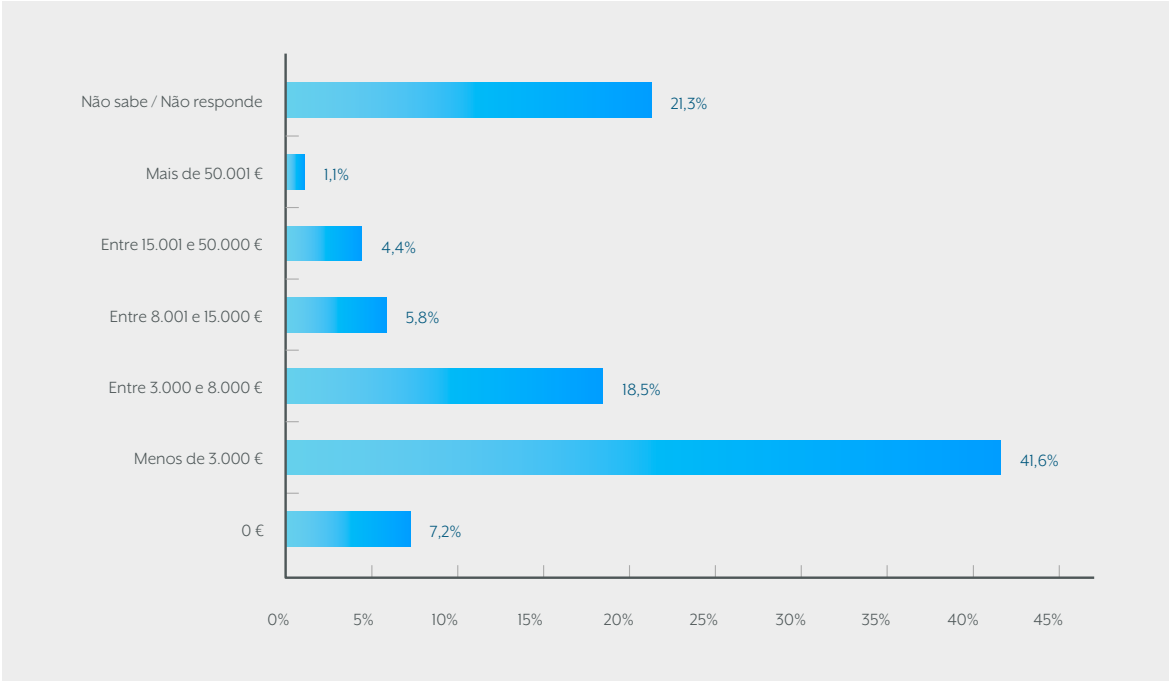
Por sectores, entre as empresas que dedicam menos de 3.000 euros a funções de cibersegurança desatacam-se as do sector da construção (45,7%). Neste sector apenas 22,2% das empresas dedicam mais de 3.000 euros a estas funções e só 1,2% mais de 50.000 euros.

Figura 5.6 – Orçamento anual de Cibersegurança, para todas as empresas, Portugal, % de empresas



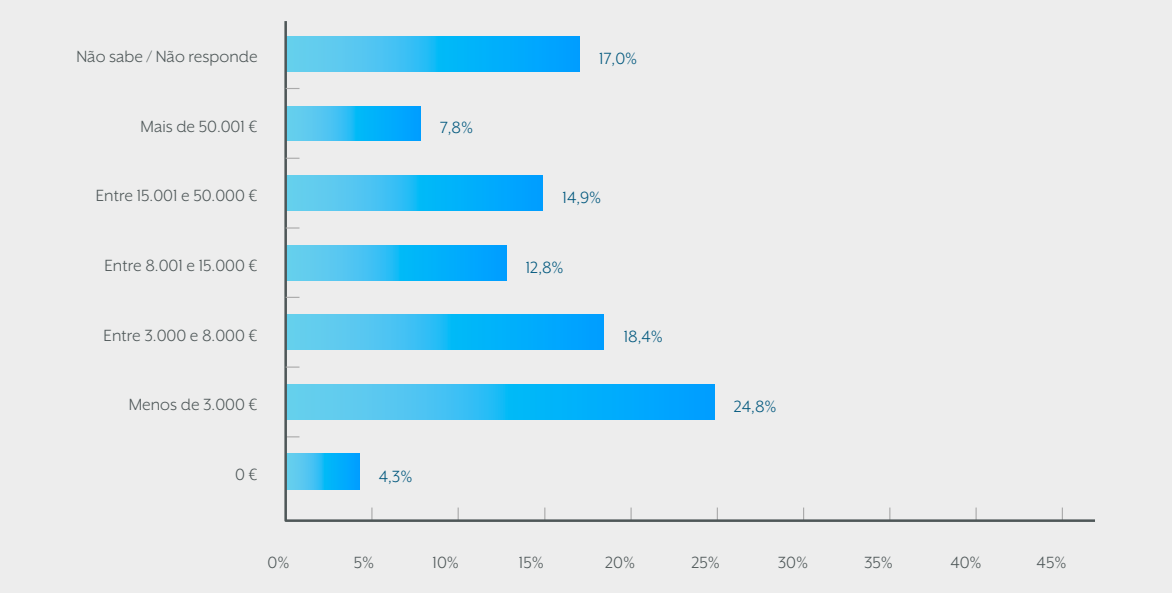
Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Figura 5.7 – Orçamento anual de Cibersegurança das pequenas empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Figura 5.8 – Orçamento anual de Cibersegurança das médias empresas, Portugal, % de empresass

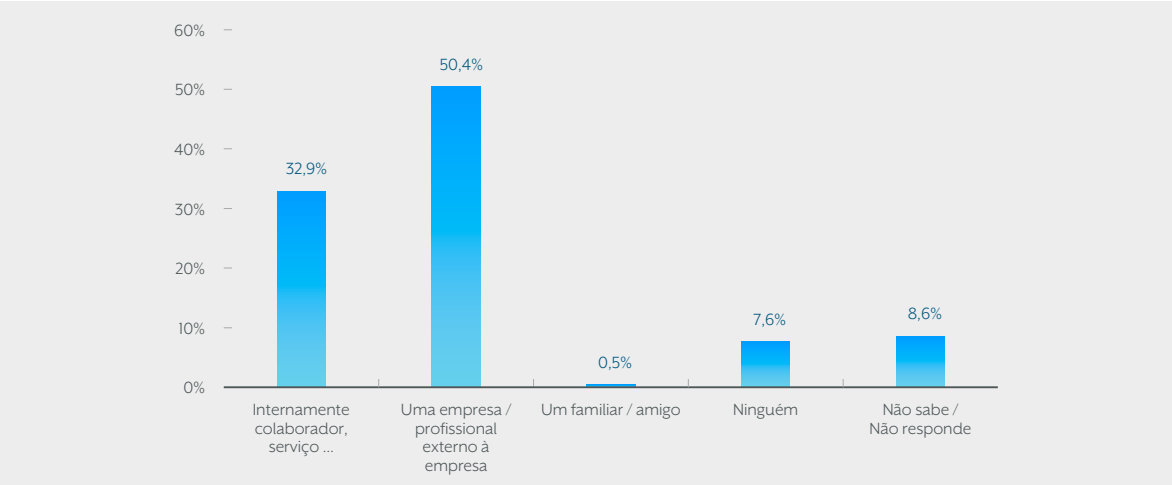


Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Contrariamente, 22,2% das empresas de serviços de elevado v.a. destinam menos de 3.000 euros à segurança TIC e 40,7% mais de 3.000. Neste sector, 11,1% das empresas têm um orçamento superior a 50.000 euros. Na indústria, a percentagem de empresas com orçamentos superiores a 3.000 euros também é bastante significativa (37,5%).

Em metade das empresas (50,4%) a gestão da cibersegurança é realizada por uma empresa especializada ou um profissional externo (Figura 5.9). Em uma em cada três empresas (32,9%), a cibersegurança é realizada internamente, utilizando recursos próprios da organização. Em 7,6% das empresas ninguém desempenha estas funções e 8,6% declara que não sabe (ou não contesta) quem o faz. Curiosamente, em uma em cada duzentas empresas a gestão da cibersegurança está nas mãos de um familiar ou de um amigo.

Figura 5.9 – Responsabilidade pela gestão de cibersegurança na empresa, para todas as empresas, Portugal, % de empresas



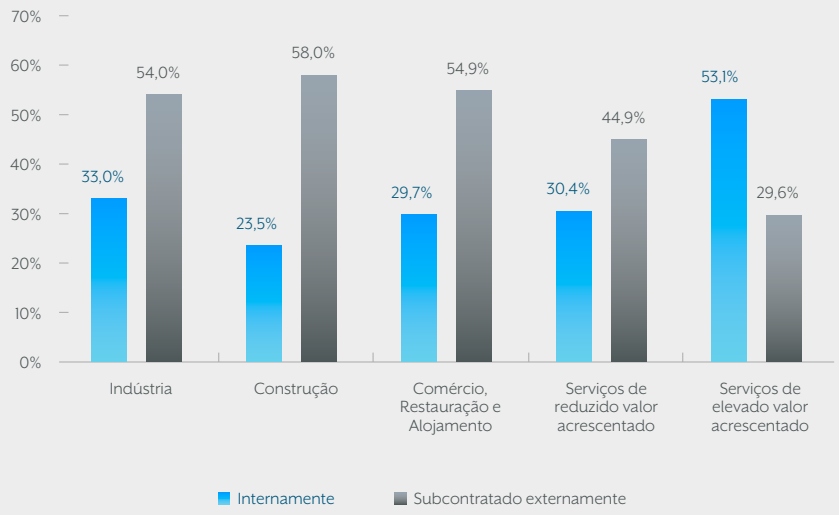
Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

À medida que o tamanho da organização aumenta observa-se uma redução do peso das respostas *Ninguém* e *Não sabe / Não responde*. A gestão informal da cibersegurança (por familiares e amigos) é marginal no caso das pequenas empresas e inexistente no das médias empresas. Nas empresas de maior dimensão ganha peso a gestão interna face ao *outsourcing* (39,0% nas médias empresas versus 30,1% nas pequenas empresas).

Por sectores, as empresas do sector dos serviços de elevado v.a têm uma preferência clara por assumir internamente as funções de cibersegurança (53,1% das empresas), recorrendo em menor media ao *outsourcing* (29,6%) (Figura 5.10). Contrariamente, no sector

da construção civil quase seis em cada dez empresas (58,0%) optam por subcontratar serviços de cibersegurança. Neste sector, só 23,5% das empresas assume internamente a gestão da mesma.

Figura 5.10 – Funções de Cibersegurança *in house* e *outsourcing*, por grandes sectores, Portugal, % de empresas



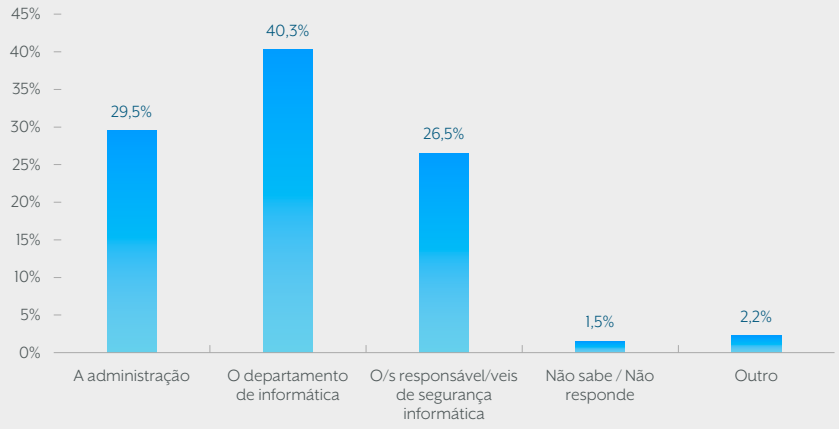
Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Embora de forma menos vincada, este padrão também domina no sector industrial e no comércio e afins. Nos serviços de reduzido v.a., embora prevaleça o *outsourcing* (44,9%), uma proporção significativa de empresas (30,4%) possui recursos próprios dedicados à segurança das TIC.

As situações de informalidade apenas se manifestam, embora marginalmente, nos sectores dos serviços de elevado v.a. e do comércio e afins. O peso das respostas *Não sabe / Não responde* situam-se à volta de 10%, exceto no caso dos serviços de elevado v.a. (1,2%).

Nas empresas que realizam internamente a gestão da cibersegurança, a responsabilidade é atribuída a diversos agentes ou departamentos (Figura 5.11). Em 40,3% das empresas a gestão é afeta ao departamento de informática e em 26,5% corresponde ao/s responsável/eis de segurança informática. Em 29,5% das empresas a administração assume a gestão da segurança cibernética.

Figura 5.11 – Responsabilidade pela gestão da Cibersegurança nas empresas em que é realizada internamente, todas as empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

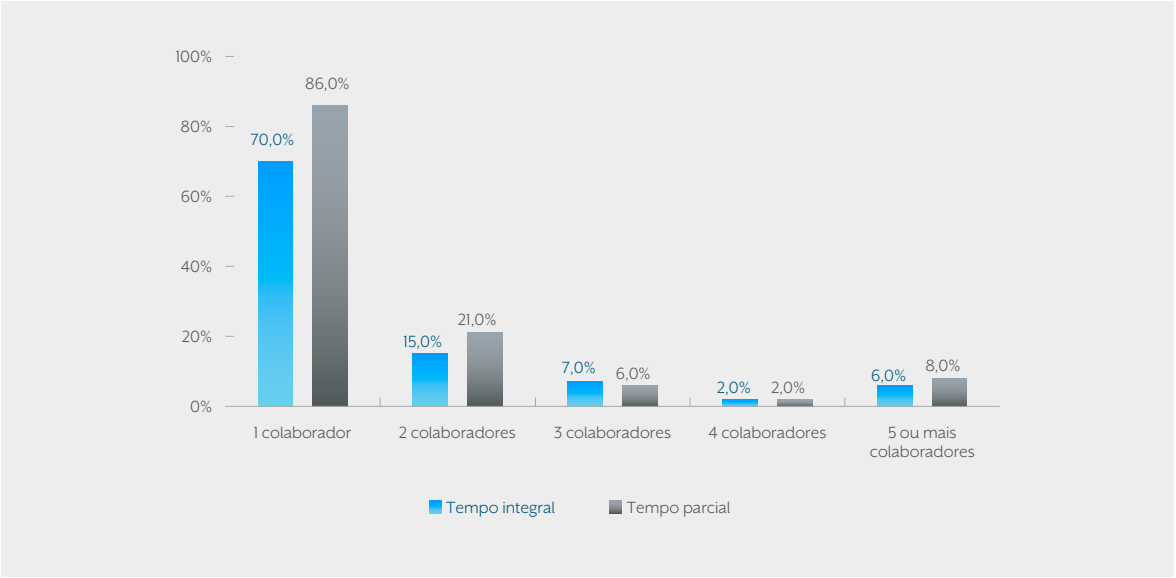
Nas empresas de maior dimensão a gestão da cibersegurança é, em grande medida, efetuada pelo departamento de informática e, em menor medida, pela administração. Nas médias empresas, em mais de metade das organizações (54,8%) a responsabilidade

da segurança das TIC corresponde ao departamento de informática, em uma em cada cinco (21,9%) ao/s responsável/eis de segurança informática e em uma em cada quatro, aproximadamente, à administração (23,3%). Nas pequenas empresas, o papel da administração é maior (28,3% das empresas) e a do departamento de informática menor (35,2%), provavelmente porque em muitos casos nem sequer existe formalmente.

A responsabilidade da cibersegurança internamente difere consideravelmente entre sectores. Os departamentos de informática são especialmente relevantes nos sectores industrial (45,1% das empresas) e no de serviços de reduzido v.a. (43,3% das empresas). No sector de serviços de elevado v.a., as empresas confiam maioritariamente as suas funções de cibersegurança ao/s responsável/eis de segurança informática (35,0% das empresas) – muito acima dos restantes sectores, exceto do sector da construção. Embora não seja a opção maioritária em nenhum caso, a administração assume as funções de segurança de TIC em 33,3% das empresas de serviços de reduzido v.a. e em 31,8% das empresas de construção. Nos restantes sectores, esta alternativa tem uma expressão menor.

Os recursos humanos afetos a tarefas relacionadas com a cibersegurança variam consideravelmente entre as empresas que realizam a gestão da segurança das TIC internamente (Figura 5.12): 70,0% das empresas conta com um colaborador a tempo integral, 15,0% com dois, 7,0% com três colaboradores e 2,0% com quatro. Uma em cada vinte empresas, aproximadamente (6%), têm cinco ou mais colaboradores dedicados à cibersegurança.

Figura 5.12 – Colaboradores encarregues da Cibersegurança, a tempo integral e a tempo parcial, para todas as empresas, Portugal, % de empresas com trabalhadores dedicados a funções de segurança TIC internamente



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

A percentagem de empresas que têm um colaborador a tempo completo é maior entre as médias que entre as pequenas (79,4% versus 72,9%). Entre as pequenas empresas, 24,0% têm dois colaboradores, enquanto que entre as médias, só 5,9% possuem esse número. Este aparente paradoxo poderá ser explicado porque muitas das empresas que operam em sectores com maiores riscos têm dimensões ainda relativamente reduzidas. Apenas 6,0% das pequenas empresas têm três ou mais colaboradores a tempo completo dedicados à segurança das TIC, enquanto 14,7% das médias empresas ultrapassam os três colaboradores nesse âmbito funcional.

Aproximadamente oito em cada dez empresas dos sectores da construção e do comércio e afins, com trabalhadores próprios para desempenhar internamente as funções de cibersegurança, têm apenas um colaborador. Para as empresas de serviços de elevado v.a. essa proporção é de seis em cada dez. As empresas deste sector destacam-se por ser as que têm mais trabalhadores a tempo integral para o desempenho destas funções (15,8% têm dois colaboradores; 10,5%, três colaboradores; 5,3%, quatro colaboradores; e, 15,8%, cinco ou mais colaboradores).

As empresas também recorrem a colaboradores a tempo parcial para desempenhar as funções de cibersegurança: 86% das empresas têm um colaborador e 21% dois colaboradores nesse regime. Entre as pequenas e as médias empresas não existem grandes diferenças

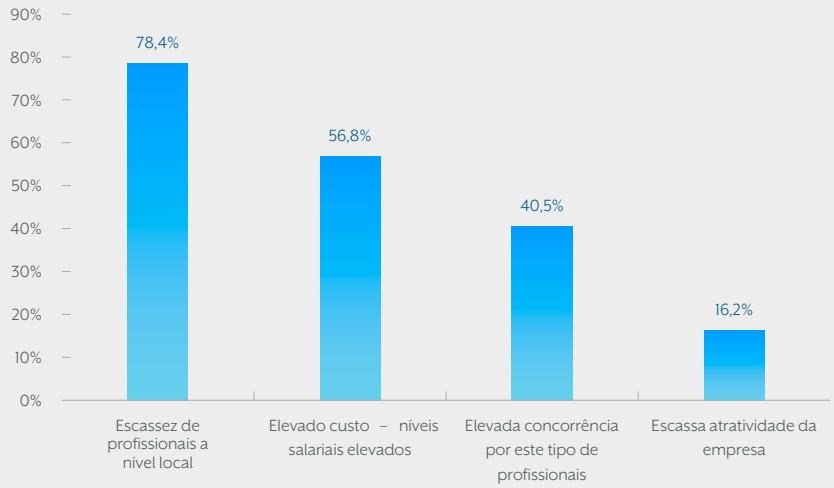
em termos de contratação a tempo parcial – as percentagens de empresas que contratam um ou dois trabalhadores nessa modalidade são muito similares. A diferença mais significativa é que, em termos relativos, mais médias empresas têm mais colaboradores a tempo parcial. Na análise sectorial apenas existem diferenças face às contratações a tempo completo, com as empresas do sector de serviços de elevado v.a. a liderar as contratações de mais de um trabalhador. Os sectores em que mais empresas contratam apenas um trabalhador a tempo parcial são a indústria, a construção e o comércio e afins.

Relativamente à capacidade das empresas para contratar/reter trabalhadores dedicados a tarefas de cibersegurança, quase uma em cada seis empresas (17,5%) manifesta que enfrenta dificuldades neste domínio. Pouco mais de três em cada dez (31,3%) declara que não tem sentido essas dificuldades. Aproximadamente, metade das empresas (51,2%) não se manifesta sobre esta questão – *Não sabe / Não responde*. Em geral, as empresas de menor dimensão, as micro e as pequenas empresas, sentem mais dificuldades para contratar/reter trabalhadores nesta área que as empresas médias.

Por sectores, três em cada dez empresas (30,2%) de serviços de elevado v.a. e uma em cada quatro do sector do comércio e afins (24,1%) reportam dificuldades para contratar. Nos restantes sectores as proporções são inferiores. As empresas do sector industrial (36,4% das empresas) e do sector dos serviços de reduzido v.a. (33,3% das empresas) são as que menos dificuldades têm sentido, quer para contratar, quer para reter colaboradores.

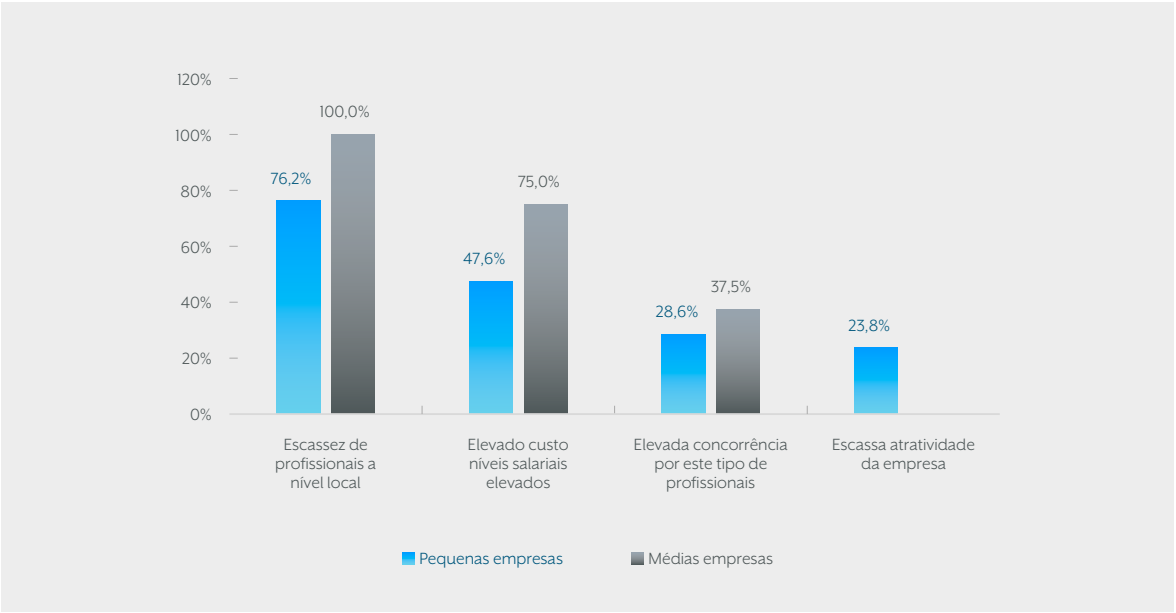
Os principais motivos reportados pelas empresas para explicar a dificuldade em contratar profissionais dedicados à cibersegurança são a escassez de profissionais a nível local (78,4%) e o seu elevado custo (56,8%) (Figura 5.13). Quatro em cada dez empresas (40,5%) consideram que a elevada concorrência nesse âmbito também afeta a contração e a retenção. Aproximadamente uma em cada seis empresas (16,2%) entende que a escassa atratividade da empresa condiciona o recrutamento e manutenção de profissionais de segurança das TIC.

Figura 5.13 – Motivos que dificultam a contratação de profissionais dedicados à Cibersegurança, para todas as empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Figura 5.14 – Motivos que dificultam a contratação de profissionais dedicados à Cibersegurança, por dimensão empresarial, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

A escassez de profissionais é reportada como um entrave à contratação/retenção de profissionais por aproximadamente a mesma percentagem de pequenas empresas que na amostra total (76,2% e 78,4%, respetivamente) (Figura 5.14). A percentagem de pequenas empresas que consideram o custo dos profissionais (47,6%) e a concorrência pelos mesmos (28,6%) condicionantes à contratação/retenção é menor que a da amostra de todas as empresas (56,8% e 40,5%, respetivamente). Contrariamente, a escassa atratividade da empresa é mais relevante para as pequenas empresas (23,8%) que para a amostra de todas as empresas (16,2%).

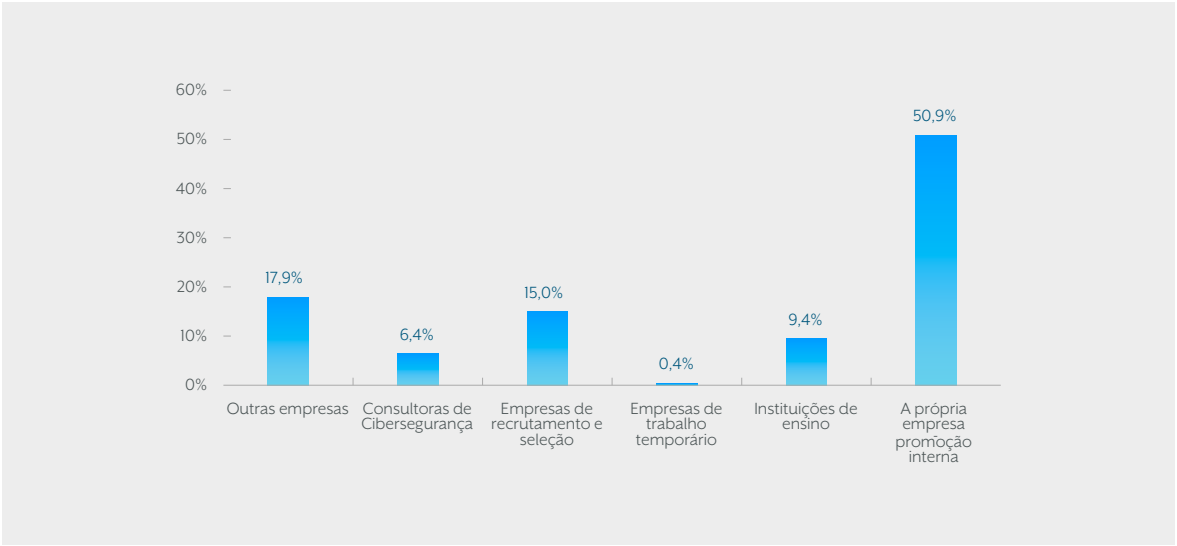
Todas as empresas médias inquiridas consideram a falta de profissionais a nível local como um condicionante à contratação e nenhuma reporta a falta de atratividade da empresa como um fator limitativo. Adicionalmente, três em cada quatro (75,0%) e pouco mais de um terço (37,5%) das empresas médias apontam que os elevados salários destes profissionais e a elevada concorrência, respetivamente, são um entrave à contratação de profissionais de segurança das TIC. A proporção de pequenas empresas que reportam cada uma das motivações referidas é inferior à das médias empresas.

A escassez de profissionais a nível local é o motivo mais importante para explicar as dificuldades de contratação entre as empresas dos sectores do comércio e afins (92,9% das empresas) e de serviços de elevado v.a. (84,6% das empresas). As empresas deste último sector também consideram importantes o elevado custo destes profissionais (76,9%) e a elevada concorrência existente no mercado pelos mesmos (69,2%). Estes dois fatores são assinalados pela totalidade das empresas de serviços de reduzido v.a. As empresas industriais apontam como motivos mais relevantes a escassez de profissionais a nível local (50,0%) e os elevados salários dos profissionais da cibersegurança (33,3%).

Os profissionais que exercem funções relacionadas com a cibersegurança nas empresas procedem maioritariamente da própria empresa (50,9%) (Figura 5.15). Acedem a essas posições por promoção interna ou mobilidade funcional. Quase 18% dos trabalhadores recrutados para trabalhar na área da segurança das TIC procedem de outras empresas; 15,0% são contratados através de empresas de recrutamento e seleção; e apenas 0,4% procedem de empresas de trabalho temporário. As empresas também recrutam diretamente em instituições de ensino superior (9,4%) e em consultoras de cibersegurança (6,4%).

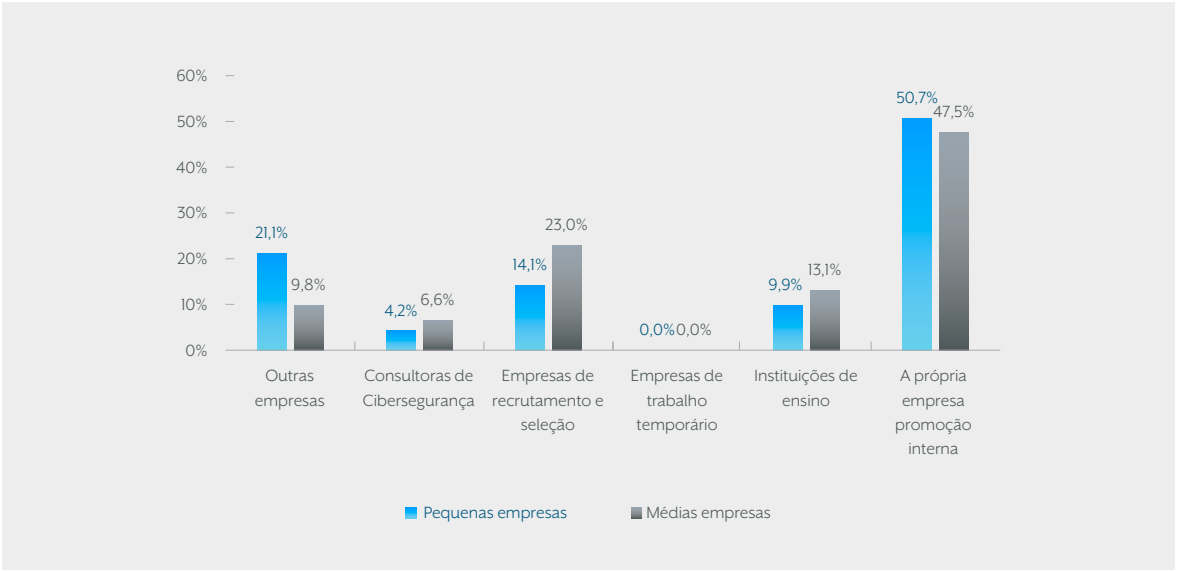
Nesta dimensão existem algumas diferenças em função do tamanho das empresas (Figura 5.16). As pequenas empresas recorrem mais que as médias ao recrutamento interno (50,7% nas pequenas empresas versus 47,5% nas médias empresas) e ao recrutamento noutras empresas (21,1% nas pequenas empresas versus 9,8% nas médias empresas). Contrariamente, as empresas médias preferem contratar através de empresas de recrutamento e seleção (23,0% nas médias empresas versus 14,1% nas pequenas empresas), nas instituições de ensino superior (13,1% nas médias empresas versus 9,9% nas pequenas empresas) e nas consultoras de cibersegurança (6,6% nas médias empresas versus 4,2% nas pequenas empresas).

Figura 5.15 – Principais fontes de recrutamento de profissionais de Cibersegurança, para todas as empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Figura 5.16 – Principais fontes de recrutamento de profissionais de Cibersegurança, por dimensão empresarial, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

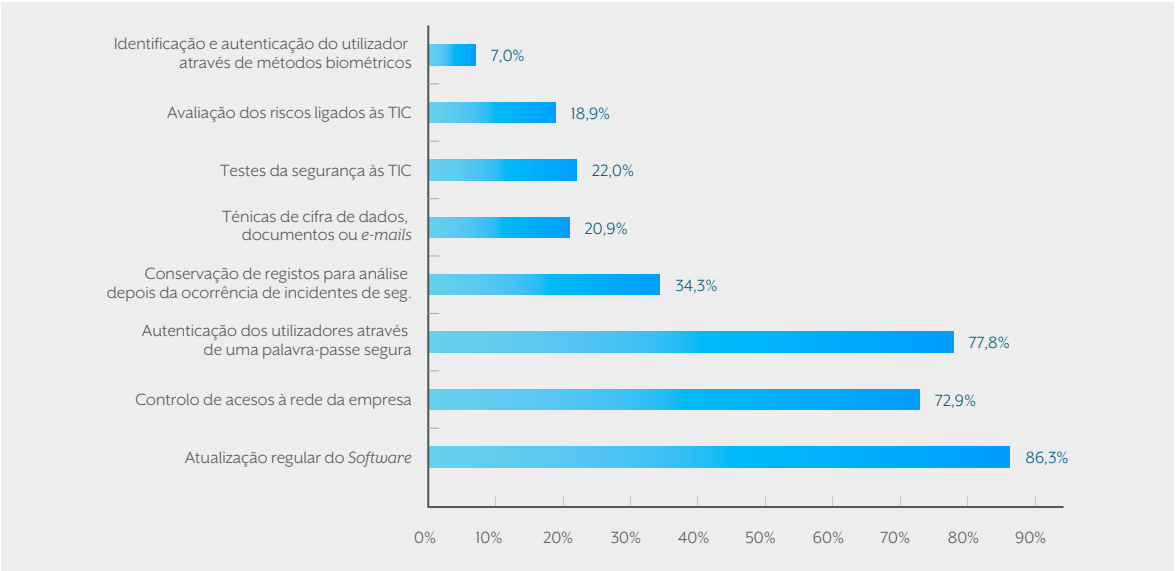
A nível sectorial, a promoção interna é dominante em todos os sectores, especialmente na construção (72,2% das empresas) e nos serviços de elevado v.a. (52,5% das empresas). As empresas de recrutamento e seleção são particularmente importantes no sector do comércio, restauração e alojamento (21,5% das empresas) e no de serviços de elevado v.a. (15,3% das empresas). As empresas de trabalho temporário apenas têm alguma relevância, embora marginal, entre as empresas de serviços de reduzido v.a. (4,3% das empresas).

As principais medidas de segurança das TIC utilizadas pelas empresas inquiridas são a atualização regular do *software* (86,3%), a autenticação dos utilizadores através de palavras-passe seguras (77,8%) e o controlo de acessos à rede da empresa (72,9%) (Figura 5.17). Um terço das empresas (34,3%) conserva os registos para análise depois da ocorrência de incidentes de segurança e um quinto (20,9%) utiliza técnicas de cifra de dados, documentos ou *e-mails*. Os testes de segurança TIC e a avaliação dos riscos ligados às TIC são medidas adotadas por 22,0% e 18,9% das empresas, respetivamente. Apenas 7,0% das empresas recorrem à identificação e autenticação do utilizador através de métodos biométricos.

Com o aumento da sua dimensão, a percentagem de empresas que adotam cada uma das medidas de segurança das TIC consideradas é superior (Figuras 5.18 e 5.19). As maiores diferenças são no controlo de acessos à rede da empresa (71,0% nas pequenas versus 84,4% nas médias), na conservação de registos para análise posterior de incidentes (30,6% versus 48,2%), na avaliação de riscos ligados às TIC (15,0% versus 30,5%) e na identificação e autenticação do utilizador mediante métodos biométricos (4,4% versus 14,4%). A atualização regular do *software* e a autenticação através de uma palavra-passe segura são medidas generalizadas nas empresas e, embora existam diferenças em função da dimensão, as diferenças na adoção destas práticas entre empresas pequenas e médias é relativamente reduzida.

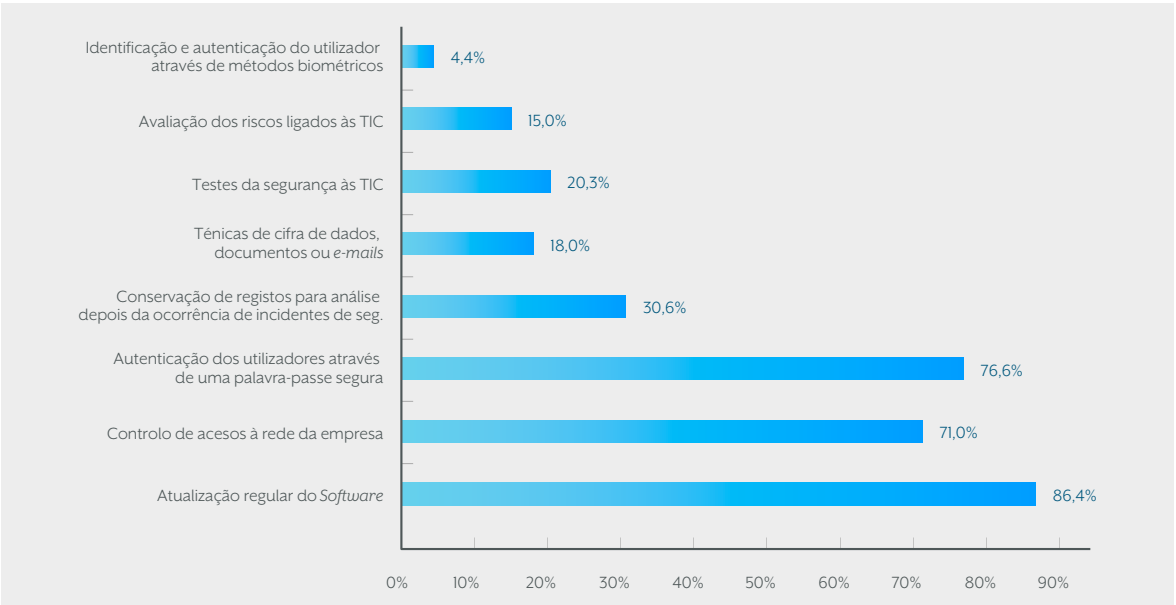
Em geral as empresas de construção são as que, em termos relativos, menos aderem às medidas de segurança das TIC. Contrariamente, estas medidas têm uma elevada penetração entre as empresas de serviços de elevado v.a. A adoção de medidas de segurança mais sofisticadas[74] é significativamente superior neste tipo de empresas. As medidas menos sofisticadas têm maior adesão nas empresas dos sectores do comércio, da restauração e do alojamento. Para além de nos serviços de elevado v.a. (9,9% das empresas), a identificação e autenticação do utilizador através de métodos biométricos tem alguma relevância nas empresas industriais (9,0%).

Figura 5.17 – Principais medidas de segurança das TIC utilizadas, para todas as empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

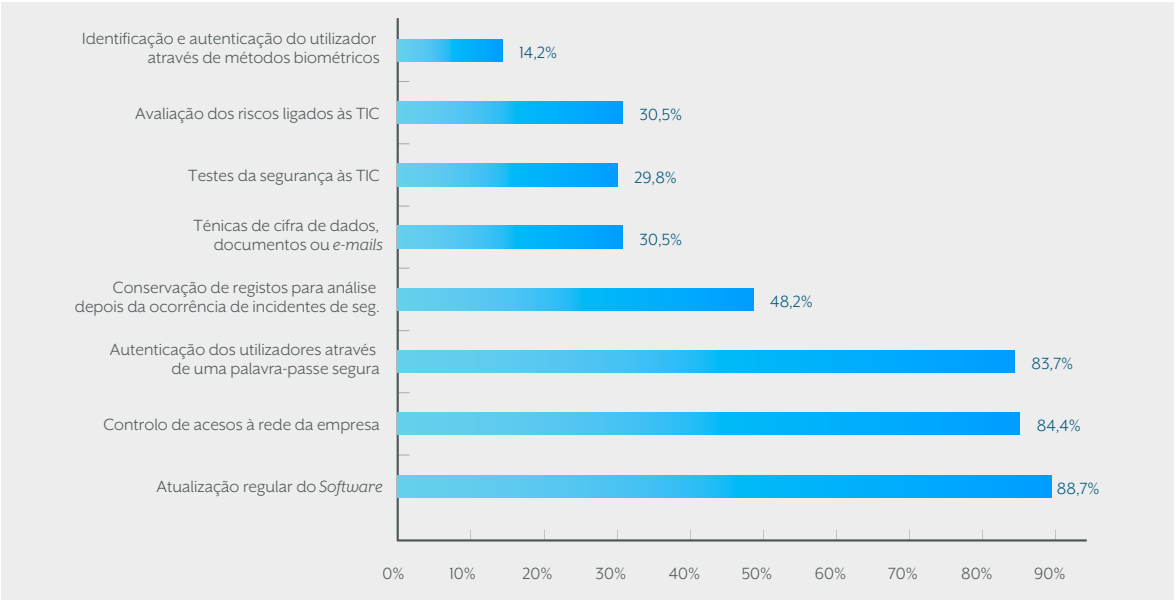
Figura 5.18 – Principais medidas de segurança das TIC utilizadas nas pequenas empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

74. Neste caso, identificação e autenticação do utilizador através de métodos biométricos, avaliação dos riscos ligados às TIC, testes de segurança às TIC, técnicas de cifra de dados, documentos ou *e-mails* e conservação de registos para análise posterior.

5.19 – Principais medidas de segurança das TIC utilizadas nas médias empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

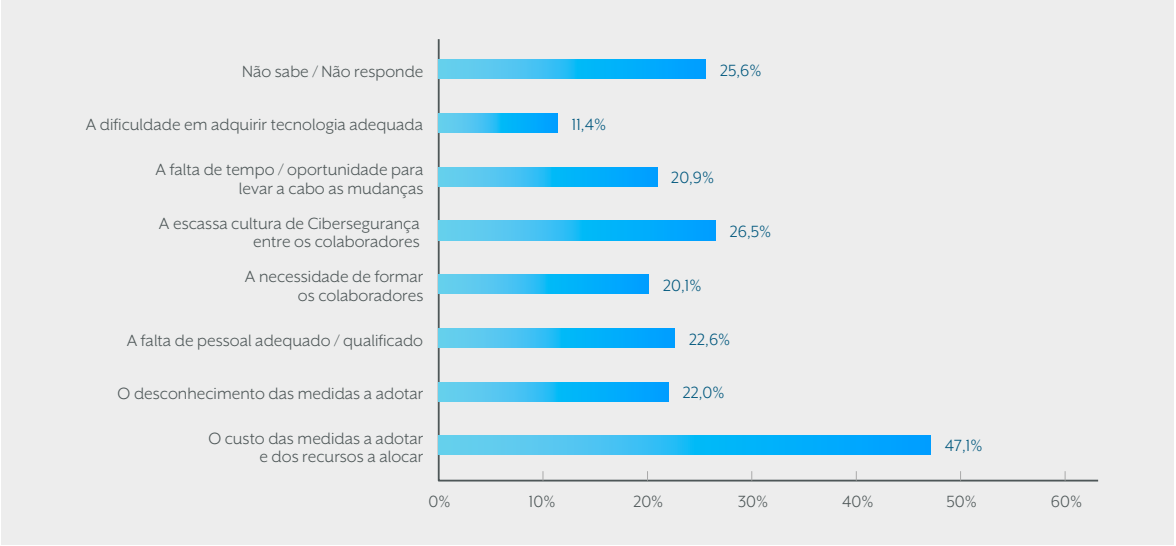
Para quase metade das empresas (47,1%) a principal barreira à implementação de medidas para melhorar os níveis de cibersegurança é o custo das mesmas e dos recursos a alocar (Figura 5.20). Outros aspetos destacados neste âmbito são a escassa cultura de cibersegurança dos colaboradores (26,5%), a falta de pessoal adequado / qualificado (22,6%) e o desconhecimento das medidas a adotar (22,0%). Uma em cada cinco empresas, aproximadamente, refere outros fatores que dificultam a implementação de medidas de segurança TIC, tais como a falta de tempo / oportunidade para levar a cabo as mudanças (20,9%) ou a necessidade de formar os colaboradores (20,1%). Uma barreira com menor relevância para as empresas é a dificuldade para adquirir tecnologia adequada (11,4%). Aproximadamente um quarto das empresas (25,6%) não sabe (não responde) quais são as principais barreiras neste âmbito.

Para as médias empresas, o custo das medidas é mais relevante que para as pequenas empresas (53,9% versus 44,2%) (Figura 5.21 e Figura 5.22). A escassa cultura de cibersegurança, a dificuldade para adquirir tecnologia adequada e a falta de pessoal adequado / qualificado também parecem ter maior relevância para as médias empresas (31,2% versus 25,5%, 15,6% versus 10,5% e 24,8% versus 22,4%, respetivamente). Nas restantes dimensões não existem diferenças significativas em função da dimensão empresarial.

Por sectores, o custo das medidas a adotar e dos recursos a alocar é invocado como uma barreira maioritariamente por empresas de serviços de elevado v.a. (60,5%) e empresas industriais (47,5%). A escassa cultura de cibersegurança é considerada uma barreira à adoção de medidas especialmente por empresas de serviços de reduzido v.a. (33,3%) e da indústria (30,5%). A falta de tempo/ oportunidade é assinalada sobretudo pelas empresas de serviços de elevado v.a. (40,7%) e a falta de pessoal qualificado (34,8%), a necessidade de formar os colaboradores (27,5%) e o desconhecimento das medidas a adotar (26,1%) pelas empresas de serviços de reduzido v.a. A dificuldade em adquirir tecnologia é sentida maioritariamente pelas empresas dos sectores do comércio, restauração e alojamento (13,3%).

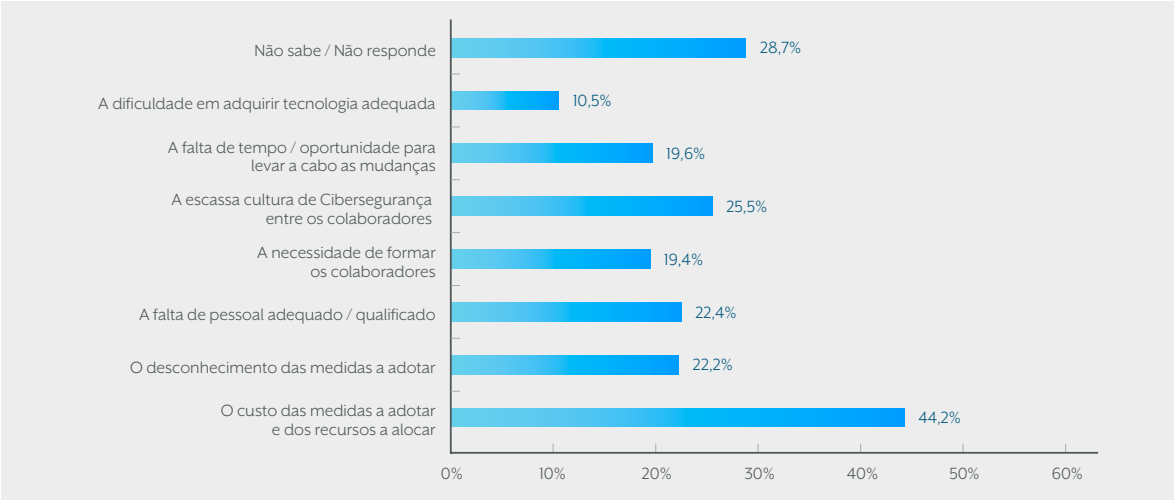
Para além do custo, as principais barreiras à implementação de medidas para melhorar os níveis de cibersegurança estão relacionadas com a escassez de profissionais e o défice de formação. Em 56,9% das empresas não existem ações de formação e sensibilização em matérias relacionadas com a cibersegurança (Figura 5.23). Em cerca de um terço das empresas (32,3%), os colaboradores têm entre uma e cinco horas de formação por ano. Uma proporção marginal de empresas disponibiliza aos seus colaboradores entre seis e dez horas de formação e mais de dez horas de formação (5,6% e 5,1%, respetivamente).

Figura 5.20 – Principais barreiras para melhorar o nível de Cibersegurança, para todas as empresas, Portugal, % de empresas



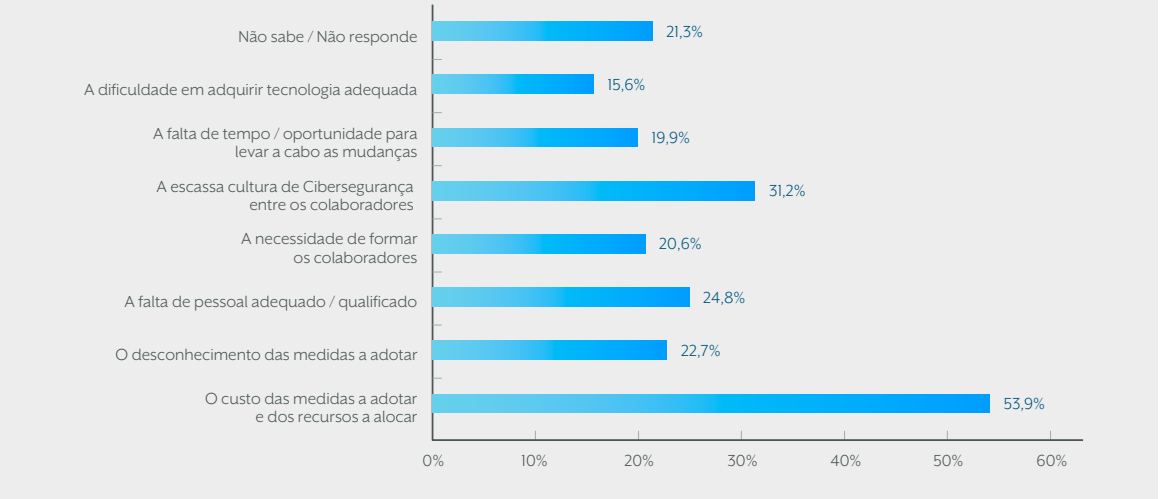
Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Figura 5.21 – Principais barreiras para melhorar o nível de Cibersegurança nas pequenas empresas, Portugal, % de empresas



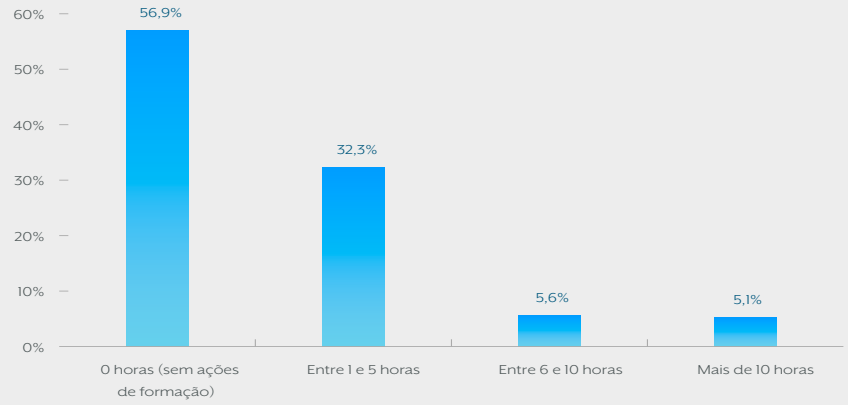
Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Figura 5.22 – Principais barreiras para melhorar o nível de Cibersegurança nas médias empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Figura 5.23 – Número de horas em ações de formação e sensibilização em matérias de Cibersegurança, para todas as empresas, Portugal, % de empresas



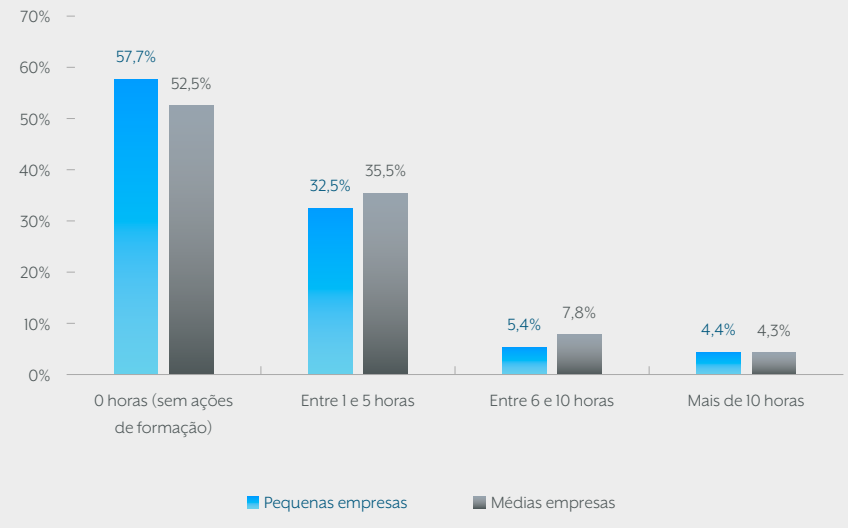
Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Nas pequenas empresas a percentagem de empresas onde os colaboradores não frequentam qualquer ação de formação é maior em 5 pontos percentuais que nas médias empresas (Figura 5.24). A proporção de empresas que fornecem aos seus colaboradores mais de dez horas de formação e sensibilização em matéria de cibersegurança é muito similar (4,4% nas pequenas versus 4,3% nas médias). A percentagem de empresas médias que disponibilizam aos colaboradores ações de formação e sensibilização de dez ou menos horas é maior do que nas pequenas empresas (43,3% nas médias versus 37,9% nas pequenas).

Nos sectores da indústria e dos serviços de reduzido v.a., as empresas em que os trabalhadores não têm qualquer ação de formação e sensibilização é superior a 60% (60,6% e 62,3%, respetivamente). Nestes sectores, as percentagens de trabalhadores com entre 1 e 5 horas de formação são as mais reduzidas dos sectores analisados, sendo iguais ou inferiores a 30%.

No sector dos serviços de elevado v.a., as empresas declaram que 11,1% dos trabalhadores recebem mais de 10 horas de formação e 9,9% entre 6 e 10 horas de formação. Neste sector, a percentagem de empresas onde os trabalhadores recebem mais de 5 horas de formação é pelo menos o dobro da dos restantes sectores.

Figura 5.24 – Número de horas em ações de formação e sensibilização em matérias de Cibersegurança, por dimensão empresarial, Portugal, % de empresas



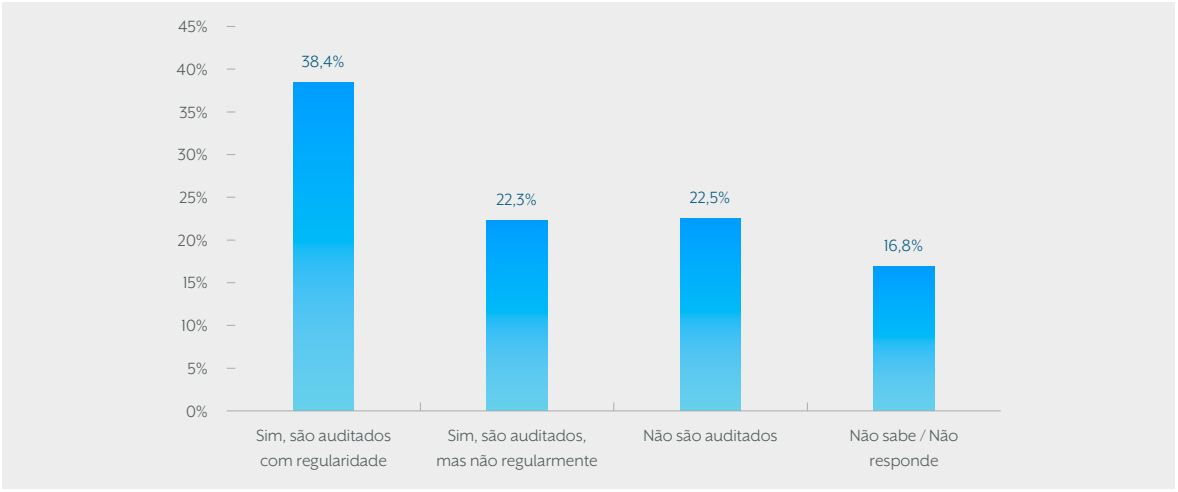
Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Um aspeto relacionado com a disponibilidade de profissionais e a sua qualidade é a certificação. Relativamente a esta questão, apenas 4,2% das empresas ou dos seus colaboradores possuem alguma certificação em matéria de cibersegurança. Quase quatro em cada cinco (78,3%) não possuem qualquer certificação. Quase uma em cada seis empresas (16,8%) não sabe ou não responde. Nas pequenas empresas, só dispõem de certificações próprias ou dos seus empregados 2,8% do total, enquanto nas médias a percentagem aumenta para 5,7%. As empresas dos sectores de serviços de elevado v.a. (8,6%) e de reduzido v.a. (7,6%), assim como as de comércio e afins (4,6%) são as que possuem mais certificações em matéria de cibersegurança, em termos relativos.

Uma outra medida de credibilização face ao exterior é a realização de auditorias às redes e sistemas de informação. Quase quatro em cada dez empresas (38,4%) realiza estas auditorias com regularidade e pouco mais de uma em cada cinco (22,3%) as leva a cabo, mas não regularmente (Figura 5.25). Mais de um quinto das empresas (22,5%) não faz auditorias às suas redes e sistemas de informação.

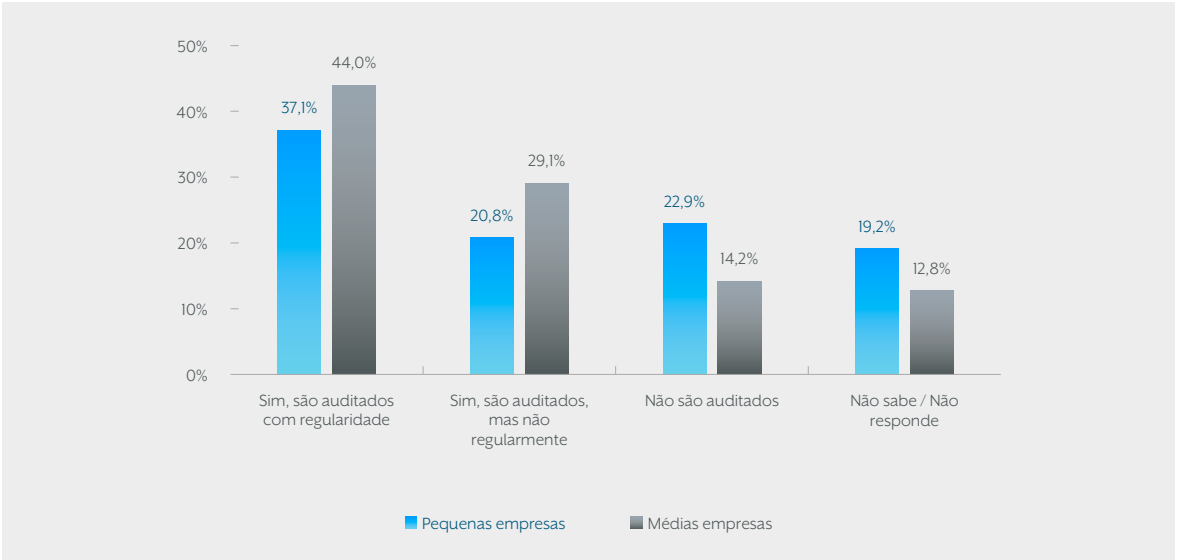
Em matéria de auditorias, as pequenas empresas quase replicam os resultados da amostra total (Figura 5.26). No caso das médias empresas os resultados são bastante diferentes. Quase 75% das empresas deste grupo auditam as suas redes e sistemas de informação, face a pouco mais de 60% para o conjunto da amostra.

Figura 5.25 – Auditorias às redes e sistemas de informação, para todas as empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Figura 5.26 – Auditorias às redes e sistemas de informação, por dimensão empresarial, Portugal, % de empresas



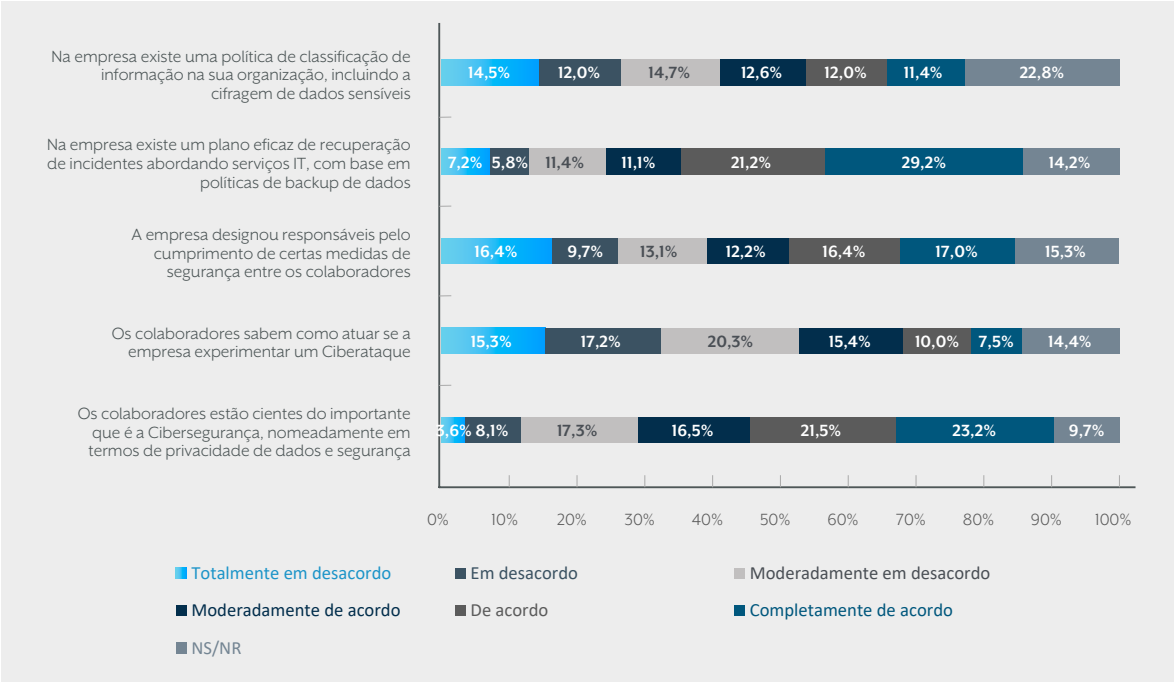
Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Em 44,0% das médias empresas as suas redes e sistemas são regulamente auditados, enquanto em 29,1% ocorre apenas de forma pontual. Apenas em 14,2% das médias empresas as redes e sistemas não são auditados.

As redes e sistemas de segurança são auditados regularmente em 44,0% das empresas do sector de serviços de elevado v.a. e em 40,5% do sector comercial, da restauração e afins. Nos restantes sectores a proporção de empresas que realizam este tipo de auditorias com frequência é menor e as que as fazem executam-nas com menor regularidade. Os sistemas de segurança não são auditados em 28,4% das empresas de construção e em 27,5% das empresas de serviços de reduzido v.a. Nos restantes sectores o peso das empresas que não realizam auditorias é menor.

Uma outra barreira relevante para a implementação de medidas de cibersegurança nas organizações é a escassa cultura de cibersegurança. Neste âmbito, as empresas consideram que existem dimensões que estão bastante desenvolvidas e outras que ainda são relativamente deficitárias (Figura 5.27). Entre as primeiras destaca-se o entendimento das empresas de que os seus colaboradores estão cientes da importância da cibersegurança, nomeadamente em termos de privacidade de dados e segurança (61,2% das respostas no espectro da concordância,[75] com 9,7% de respostas não sabe, não responde) e de que dispõem de planos eficazes de recuperação de incidentes, com base em políticas de *backup* de dados (61,5% das respostas no espectro da concordância,com 14,2% de respostas não sabe, não responde).

Figura 5.27 – Grau de concordância com as afirmações relativas à cultura de Cibersegurança, para todas as empresas, Portugal, % empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

As empresas consideram que existem défices ao nível dos protocolos de atuação em caso de ciberataques (apenas 32,9% das respostas no espectro da concordância, com 14,4% de respostas não sabe, não responde) e das políticas de classificação de informação (apenas 36,0% das respostas no espectro da concordância, com 22,8% de respostas não sabe, não responde). As opiniões das empresas dividem-se em relação à existência da prática de designação de responsáveis nomeados para o cumprimento de certas medidas de segurança entre os colaboradores (apenas 45,6% das respostas no espectro da concordância e 39,1% no espectro da discordância,[76] com 15,3% de respostas não sabe, não responde).

Na análise por dimensão empresarial das várias componentes sobre a cultura de cibersegurança conclui-se que as médias empresas consideram que os seus empregados não estão tão cientes da importância de cibersegurança como seria de esperar (espectro de concordância similar, mas menos empresas completamente de acordo), que possuem uma política de classificação de informação estruturada (maior espectro de concordância e mais empresas completamente de acordo) e que dispõem de um plano de recuperação de incidentes (muito maior espectro de concordância e muitas mais empresas completamente de acordo). As empresas médias têm mais bem definida a cadeia de comando para a aplicação das medidas de segurança (maior espectro de concordância e mais empresas de acordo e completamente de acordo), mas têm dúvidas sobre se os seus colaboradores sabem como atuar em caso de ciberataque (mais repostas no espectro de concordância, mas menos completamente de acordo).

75. Moderadamente de acordo, de acordo e completamente de acordo.

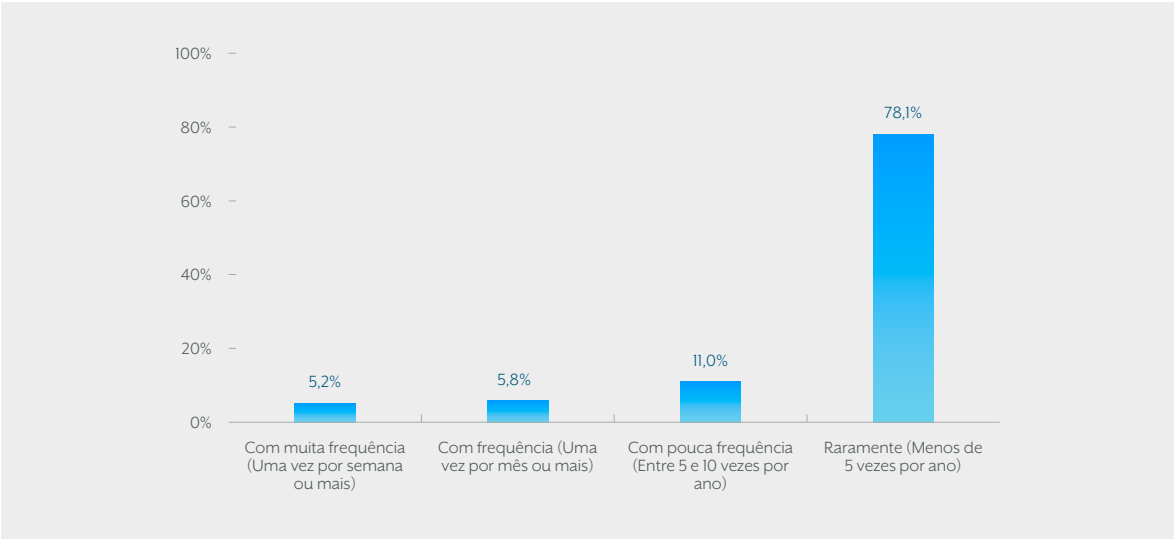
76. Totalmente em desacordo, em desacordo, moderadamente em desacordo.

As empresas de serviços de elevado v.a. julgam que os seus colaboradores estão mais cientes da importância da cultura de segurança que as dos restantes sectores e, num maior número de casos, possuem planos de recuperação de incidentes e uma política de classificação de informação estruturada (espectro de concordância maior nas três dimensões). Os empregados menos cientes da importância da cibersegurança são os das empresas industriais, e as empresas onde menos desenvolvidos estão os planos de recuperação de incidentes são as de construção (menor espectro de concordância, em ambas as dimensões). O sector da construção é, de todos os sectores, o que apresenta piores resultados nas restantes dimensões – atuação em caso de ciberataque, designação de responsáveis e política de classificação de informação (menor espectro de concordância). Nessas dimensões os resultados estão, em grande medida, alinhados com os do conjunto da amostra, exceto para o sector de serviços de elevado v.a., onde genericamente são melhores.

Das empresas inquiridas, quase um quarto (24,2%) revela ter sido alguma vez alvo de um ciberataque, enquanto que quase dois terços (64,1%) manifestam que nunca sofreram um ataque desta natureza. Quase 12% das empresas não sabem se experimentaram ou não um incidente deste tipo ou simplesmente não responderam. Entre as pequenas empresas, as vítimas de ciberataques são pouco mais de duas em cada dez (21,5%) e, entre as médias, quase três em cada dez (28,4%). Nunca sofreram ciberataques duas em cada três pequenas empresas (67,1%) e seis em cada dez (58,9%) médias empresas. A percentagem de empresas que indicaram a opção *Não sabe / Não responde* é, no caso das pequenas e das médias empresas, similar à da amostra total.

Os sectores onde uma maior percentagem de empresas reporta ter sido alvo de um ciberataque são o comércio e afins e os serviços de reduzido v.a. (com percentagens ligeiramente superiores a 24,5%). O sector onde uma maior proporção de empresas declara não ter sido objeto de ciberataques é o dos serviços de reduzido v.a. (77,2%). Este sector é onde menos empresas indicam a opção de saída (não sabe, não responde), à volta de 3%. Nos restantes sectores esta possibilidade é assinalada por mais de 10% das empresas.

Figura 5.28 – Frequência dos incidentes de cibersegurança, para todas as empresas, Portugal, % de empresas que foram alvo de ciberataques



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Uma larga maioria das empresas experimenta um número muito reduzido de incidentes de segurança das TIC por ano (Figura 5.28). Aproximadamente 78% das empresas afirma ter menos de cinco incidentes por ano, e 11% das empresas, entre cinco e dez vezes por ano. Contrariamente, 5,8% reportam incidentes de segurança das TIC pelo menos uma vez por mês, e 5,2%, pelo menos uma vez por semana.

Nas pequenas empresas os incidentes de cibersegurança são menos frequentes. Mais de nove em cada dez destas empresas (93,5%) declaram que o número de incidentes é inferior a dez vezes por ano (7,6% entre cinco e dez vezes por ano e 85,9% menos de cinco vezes por ano). No caso das médias empresas, 92,5% reportam menos de dez incidentes por ano, mas a percentagem de empresas que sofrem entre cinco e dez incidentes é maior que no caso das pequenas (17,5%, entre cinco e dez vezes por ano e 75,0% menos de cinco vezes por ano). Curiosamente, nenhuma empresa média experimenta incidentes com muita frequência (uma vez por semana ou mais), enquanto que 3,3% das pequenas empresas sofrem incidentes com elevada frequência, o que poderá estar relacionado com a perceção de vulnerabilidade dos ciberatacantes.

As empresas da indústria e da construção são as que experimentam incidentes de cibersegurança com menor frequência (menos de dez vezes por ano em 95,6% e 95,0% dos casos, respetivamente, com menos de cinco vezes por ano em 86,7% e 80,0% dos casos, respetivamente). Contrariamente, os ataques são bastante frequentes, em termos relativos, nas empresas de serviços de elevado v.a. (27,8% das empresas com uma vez por mês ou mais, e 16,7% com uma vez por semana ou mais) e de serviços de reduzido v.a. (11,8% das empresas, com uma vez por semana ou mais).

Mais de um terço das empresas (36,8%) julga que houve um aumento dos incidentes de cibersegurança desde o início da pandemia. Para 54,2% não houve alterações neste âmbito. Quase 10% das empresas não sabem (ou não respondem) se efetivamente houve ou não um aumento no número e frequência dos ciberataques. A perceção relativa ao aumento dos incidentes de segurança das TIC é bastante superior entre as médias, em comparação com as pequenas empresas (52,5% versus 31,5%). As médias empresas também estão mais cientes da situação, dado que apenas 5,0% responde *Não sabe / Não responde*, face a 9,8% das pequenas empresas.

A maior perceção do aumento de incidentes desde o início da pandemia é entre as empresas do sector industrial (46,7%) e a menor entre as da construção (20,0%). Nos restantes sectores, uma em cada três empresas considera que os ataques aumentaram desde o início da crise pandémica. Exceto para os sectores de serviços (0% nos de elevado v.a. e 5,9% nos de reduzido v.a.), a opção de saída *Não sabe / Não responde* representa uma percentagem ligeiramente superior à da média das empresas da amostra.

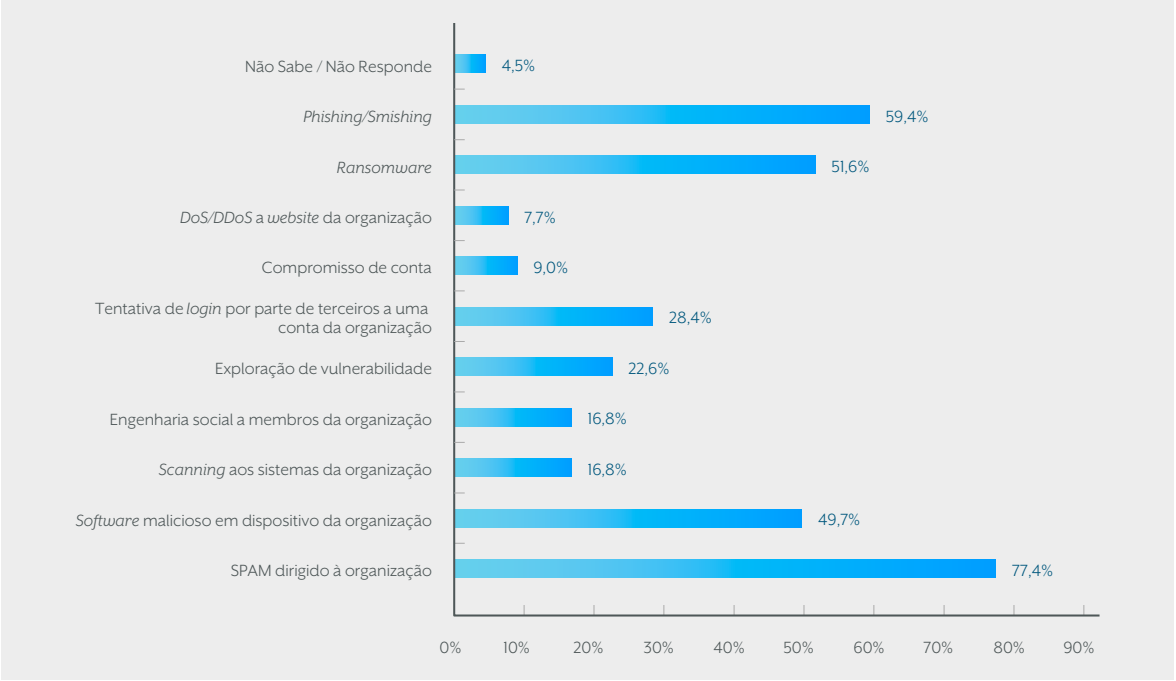
Relativamente aos custos dos incidentes de cibersegurança, dada a elevadíssima percentagem de empresas que respondem *Não sabe / Não responde* (89% das empresas que sofreram um incidente deste tipo), pode concluir-se que: i). Muitas empresas conhecem o custo médio destes incidentes, mas não o querem revelar; e, ii). Outras não conhecem o custo médio, porque, dado o seu caráter sistémico, não é fácil de calcular. Apenas 11% das empresas declara saber qual o custo médio de um incidente de cibersegurança. Esta percentagem aumenta até os 14,1% para as pequenas empresas e diminui até aos 6,7% para as médias empresas. Por sectores, 20,0% das empresas de construção e 16,7% das de serviços de elevado v.a. declaram conhecer o custo médio aproximadamente. Nos restantes sectores a percentagem é bastante menor. Na indústria apenas 6,7% das empresas reconhece conhecer o custo médio desses incidentes.

As empresas inquiridas reportam uma ampla panóplia de tipologias de incidentes (Figura 5.29). Os incidentes mais frequentes são o SPAM (77,4%), o *Phishing/Smishing* (59,4%), o *Ransomware* (51,6%) e o *software* malicioso em dispositivos (49,7%). Outros menos frequentes são as tentativas de *login* por parte de terceiros (28,4%), a exploração de vulnerabilidades (22,6%), a engenharia social a membros da organização (16,8%) e o *scanning* dos sistemas da empresa (16,8%). Uma percentagem reduzida de empresas sofreu incidentes de compromisso de conta (9,0%) e de *DoS/DdoS* a *websites* (7,7%). Na maioria das tipologias de ataques, a percentagem de médias empresas que os reportam é superior ao de pequenas empresas.

O SPAM e o *Phishing/Smishing* são muito frequentes em todos os sectores, com diferenças pouco assinaláveis entre eles. O *software* malicioso é menos frequente nas empresas da construção e do comércio e *ransomware* nas de serviços de elevado v.a. Genericamente, o resto dos incidentes são mais frequentes nas empresas do sector dos serviços e, dentro deste, especialmente nos de elevado v.a.

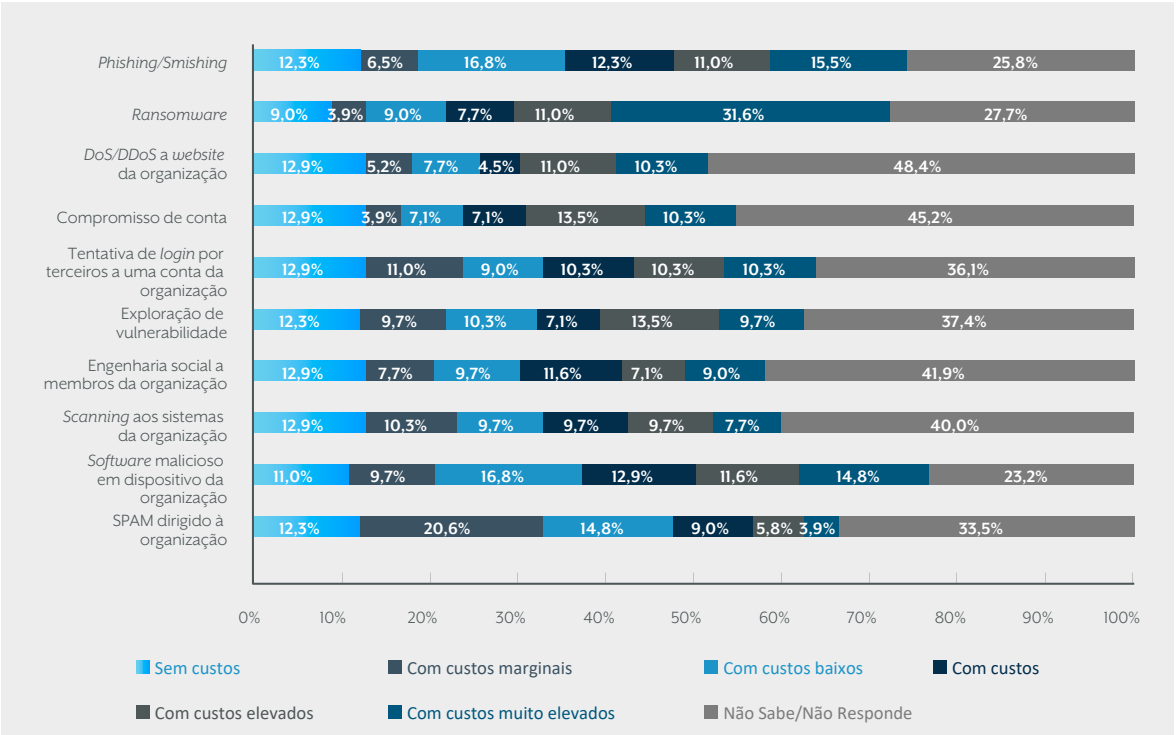
Os custos dos incidentes de segurança são percecionados de forma diferente pelas empresas (Figura 5.30). Aparentemente, as empresas conhecem melhor os custos de alguns deles, nomeadamente do *software* malicioso, do *Phishing/Smishing* e do SPAM, dado que a percentagem de empresas que respondem *Não sabe / Não responde* é bastante inferior nestes casos. Uma explicação plausível para o melhor conhecimento dos custos associados a estes incidentes poderá estar relacionada com a maior frequência com que se verificam.

Figura 5.29 – Tipologia de incidentes de segurança ou ataques sofridos, para todas as empresas, Portugal, % do total de empresas que foram alvo de ciberataques



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Figura 5.30 – Custos para a empresa das várias tipologias de incidentes, para todas as empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Apesar de que aproximadamente um quarto das empresas (27,7%) não sabe (ou não responde), as empresas parecem estar cientes dos custos associados ao *Ransomware*, dado que mais de metade (50,1%) considera que são incidentes com impacto nos custos. Do total de empresas que reportam incidentes de segurança, 31,6% associa o *Ransomware* a custos muito elevados.

Quase duas em cada cinco empresas (39,0%) também atribuem custos ao *software* malicioso. Para 14,8% das empresas este tipo de incidentes tem custos muito elevados para a organização. Das diferentes tipologias de incidentes analisadas, o SPAM é o que as empresas associam a custos mais baixos.

Nas tipologias de incidentes menos frequentes (Figura 5.29), as empresas têm mais dificuldades para pronunciar-se sobre os seus impactos nos custos – maior percentagem de respostas *Não sabe / Não responde*. Provavelmente esse desconhecimento leva a muitos dos respondentes a subavaliar os custos, dado que, em muitos casos, o espectro de respostas associado a custos para as empresas (Com custos, Com custos elevados e Com custos muito elevados) varia entre os 25% e os 30% aproximadamente.

A análise dos resultados revela que as pequenas empresas dão menos importância que as médias aos custos do SPAM (17,5% versus 22,8%) e do *ransomware* (45% versus 49,9%, com uma percentagem similar de respostas Com custos significativos). Uma outra diferença assinalável entre as pequenas e as médias empresas é que uma maior proporção destas últimas responde *Não sabe / Não responde*, o que mais uma vez pode significar a não disponibilidade para revelar ou o desconhecimento real, o que neste caso indicaria que as médias empresas estão mais cientes da dificuldade em estimar os custos efetivos de alguns destes incidentes.

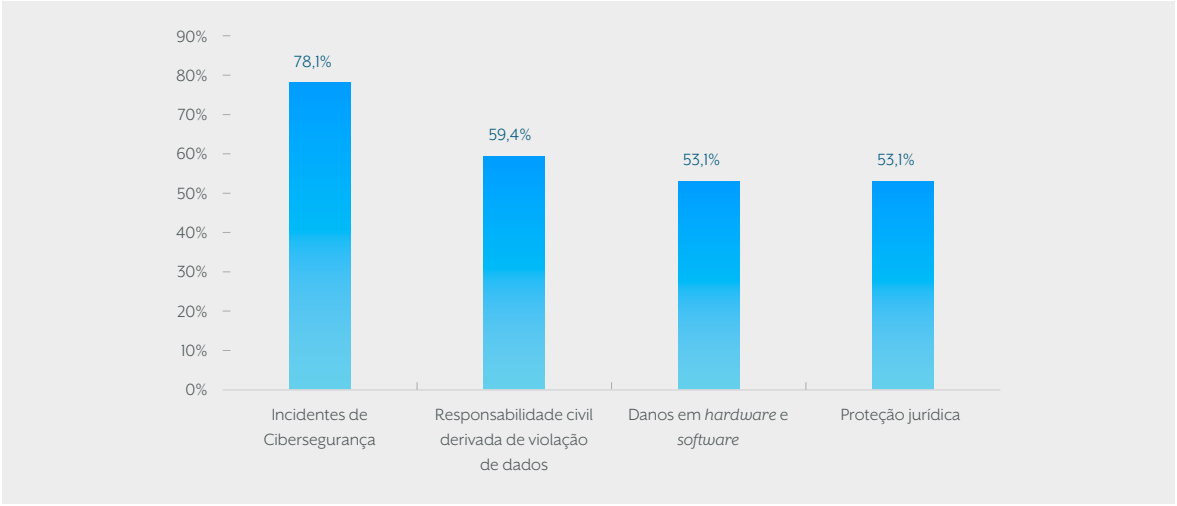
As empresas da indústria e da construção dão menos importância que a média aos custos associados a todos os incidentes de segurança, exceto aos do SPAM. Contrariamente, as de serviços de elevado v.a. dão mais importância que a média aos custos potencialmente provocados pelos incidentes de cibersegurança, exceto aos do *ransomware*. Genericamente, o padrão é similar no sector do comércio, restauração e alojamento. No sector de serviços de reduzido v.a. não há regularidades face à média.

Apenas 5,0% das empresas possuem um seguro para cobrir riscos cibernéticos. Sete em cada dez empresas (70,4%) não estão cobertas contra este tipo de riscos e uma em cada quatro (24,6%) não sabe (não responde) se dispõe deste tipo de instrumentos de proteção. À medida que aumenta a dimensão empresarial, a percentagem de empresas com estes seguros aumenta. Quase uma em cada dez médias empresas (8,5%) possui um seguro contra riscos cibernéticos (63,8% não tem), enquanto que só 4,0% das pequenas tem seguros com esta tipologia de coberturas (70,3% não tem).[77]

A contratação de seguros contra riscos cibernéticos é considerável entre as empresas de serviços de elevado v.a., 13,6% dessas empresas possuem um seguro deste tipo. Só 1,2% das empresas de construção dispõe desta tipologia de seguros. Nos restantes sectores estas coberturas são contratadas por poucas empresas (5,8% nas de serviços de reduzido v.a., 4,0% nas industriais e 3,6% nas de comércio e afins).

Apenas três em cada dez empresas (31,3%) sabem qual é a cobertura máxima do seguro; as restantes não sabem ou não respondem. O conhecimento sobre a cobertura máxima é menor entre as pequenas empresas (29,4%) e maior entre as médias empresas (33,3%). É também superior nos sectores de serviços (100,0% nos de reduzido v.a. e 54,4% nos de elevado v.a.)

Figura 5.31 – Coberturas dos seguros contra riscos cibernéticos, para todas as empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

As principais coberturas destes seguros são os incidentes de cibersegurança (nos seguros de 78,1% das empresas) e a responsabilidade civil derivada da violação de dados (nos seguros de 59,4% das empresas) (Figura 5.31). Outras coberturas incluídas nestes seguros são os danos no *hardware* e *software* e a proteção jurídica (nos seguros de 53,1% das empresas, em ambos os casos). As diferenças por dimensão empresarial não são neste caso significativas. Por sectores, não existe um padrão claramente definido, no entanto os sectores com mais coberturas são o da construção e o dos serviços de reduzido v.a.

77. As diferenças são respostas Não sabe / Não responde.

DESTAQUES CAPÍTULO V

Tal como as suas congéneres europeias, as PMEs portuguesas apresentam níveis crescentes de exposição digital, estão a intensificar os seus processos de digitalização e tendem a gerir volumes de dados privados cada vez maiores e mais diversificados. No entanto, em geral, as PMEs portuguesas estão relativamente atrás face à média da União Europeia e, especialmente, face às empresas do Norte da Europa. Em algumas dimensões, as empresas nacionais têm dificuldade para quantificar aspetos relacionados com a componente digital dos seus negócios e com as suas políticas e práticas de cibersegurança.

Quase todas as PMEs têm alguma forma de presença digital, nomeadamente páginas de Internet ou *e-mail* corporativo. Quase duas em cada três dispõem de redes sociais e uma em cada cinco plataformas de visibilização de negócios. As *apps* corporativas são ferramentas marginais nas PMEs nacionais. Pouco mais de uma em cada dez PMEs portuguesas realiza vendas *online* e menos de 6% obtêm mais de 20% do seu volume de negócios através de canais digitais.

As PMEs portuguesas processam diferentes tipologias de informação digital, nomeadamente de fornecedores e clientes. Três em cada quatro empresas processam dados pessoais ou empresariais de fornecedores e clientes e mais de metade dados bancários de fornecedores, clientes e empregados.

Para uma proporção considerável das PMEs portuguesas, a interrupção da rede ou das TIC ou a violação de dados podem dar origem a perdas financeiras significativas, a impactos relevantes na reputação ou a um risco acrescido de incumprimento de contratos.

Mais de um terço das PMEs portuguesas dedica à cibersegurança menos de 3.000 euros anuais, um terço mais de 3.000 euros e o resto não sabe (ou não responde) quanto destina a esta função. Uma em cada dez empresas tem um orçamento de cibersegurança superior a 15.000 euros anuais.

Metade das empresas subcontratam as tarefas relacionadas com a cibersegurança, enquanto que aproximadamente um terço as realiza internamente. Nestes casos, o departamento de informática ou o responsável/eis de segurança informática assumem essas tarefas na empresa.

A maioria das PMEs portuguesas (70%) têm apenas um colaborador a tempo integral dedicado às funções de cibersegurança. Metade das restantes empresas têm dois colaborares. O padrão para os colaboradores a tempo parcial é bastante similar.

Os principais motivos invocados pelas PMEs portuguesas para contratar/reter profissionais dedicados à cibersegurança é a sua escassez a nível local (78,4%) e o seu elevado custo (56,8%). As PMEs recrutam estes profissionais externamente noutras empresas (17,9%) ou através de empresas de recrutamento e seleção (15,0%), embora a opção preferida seja a promoção interna (50,9%).

As principais medidas de segurança das TIC utilizadas pelas PMEs portuguesas são a atualização regular do *software* (86,3%), a autenticação dos utilizadores através de palavras-passe seguras (77,8%) e o controlo de acessos à rede da empresa (72,9%). Um terço das empresas conserva os registos para análise após a ocorrência de incidentes de segurança e um quinto utiliza técnicas de cifra de dados, documentos ou *e-mails*. Os testes de segurança das TIC e a avaliação dos riscos ligados às TIC são menos frequentes e a identificação e autenticação do utilizador através de métodos biométricos é marginal.

Para quase metade das empresas a principal barreira à implementação de medidas para melhorar os níveis de cibersegurança é o custo das mesmas. Outros impedimentos invocados são a escassa cultura de cibersegurança dos colaboradores (26,5%), a falta de pessoal adequado / qualificado (22,6%) e o desconhecimento das medidas a adotar (22,0%).

A formação dos trabalhadores em matéria de cibersegurança é um ponto fraco das PMEs portuguesas. Quase seis em cada dez empresas não disponibilizam aos seus colaboradores ações de formação e sensibilização em matérias relacionadas com a cibersegurança. Em cerca de um terço das empresas, os colaboradores têm entre uma e cinco horas de formação por ano e em pouco mais de 10% das empresas mais de seis horas anuais (metade entre seis e dez). A certificação dos trabalhadores em matéria de cibersegurança é marginal nas PMEs portuguesas (apenas 4,2% das empresas ou dos seus trabalhadores possuem certificações deste tipo).

Outra medida de credibilização exterior, relacionada com a cibersegurança, é a auditoria de redes e sistemas de informação das empresas. Quase quatro em cada dez empresas realiza estas auditorias com regularidade e pouco mais de uma em cada cinco de forma pontual. Mais de um quinto das empresas não faz auditorias às suas redes e sistemas de informação.

Relativamente à cultura de cibersegurança nas PMEs portuguesas, as empresas, em geral, consideram que os seus colaboradores estão cientes da importância da cibersegurança, nomeadamente em termos de privacidade de dados e segurança, e que os planos de recuperação de incidentes são eficazes. Não obstante, as PMEs entendem que existem défices nos protocolos de atuação em caso de ciberataques e nas políticas de classificação de informação.

Quase um quarto das PMEs portuguesas já foi alguma vez alvo de um ciberataque, enquanto que quase dois terços nunca sofreram um ataque cibernético. Entre as empresas que experimentaram ciberataques, a maioria (78%) sofre menos de cinco incidentes por ano. Só uma em cada vinte empresas reporta pelo menos um incidente por semana. De qualquer forma, a tendência é crescente, dado que mais de um terço das empresas considera que desde o início da pandemia houve um aumento deste tipo de incidentes de segurança.

Os incidentes mais frequentes são o SPAM (77,4%), o *Phishing/Smishing* (59,4%), o *Ransomware* (51,6%) e o *software* malicioso em dispositivos (49,7%). Outros menos frequentes são as tentativas de *login* por parte de terceiros (28,4%), a exploração de vulnerabilidades (22,6%), a engenharia social a membros da organização (16,8%) e o *scanning* dos sistemas da empresa (16,8%).

Aparentemente as empresas conhecem melhor os custos do *software* malicioso, do *Phishing/Smishing* e do SPAM, provavelmente devido à sua maior incidência/frequência. Nas tipologias de incidentes menos frequentes as empresas têm menor conhecimento dos seus impactos nos custos. As PMEs portuguesas associam o SPAM a custos mais baixos. Contrariamente, associam o *Ransomware* e o *software* malicioso a custos significativos.

Apenas 5,0% das empresas possuem um seguro para cobrir riscos cibernéticos. As principais coberturas destes seguros são os incidentes de cibersegurança e a responsabilidade civil derivada da violação de dados. Outras coberturas incluídas nestes seguros são os danos no *hardware* e *software* e a proteção jurídica.

CONCLUSÕES E RECOMENDAÇÕES

CONCLUSÕES E RECOMENDAÇÕES

O maior impacto das falhas de cibersegurança ou dos ciberataques nas organizações relaciona-se com a crescente importância dos incidentes e dos ataques (abrangência e poder destrutivo) e com o incremento da sua probabilidade de ocorrência (expansão dos agentes maliciosos e aumento da frequência). Os riscos cibernéticos continuam a ser um dos principais riscos quer a curto, quer a médio prazo, tanto globalmente como para as entidades nacionais. Embora as empresas tenham um papel fundamental na gestão e minimização desses riscos, a intervenção dos governos e das entidades estatais nesta matéria é incontornável, nomeadamente em âmbitos como a capacitação institucional, a governança e a regulação.

Nos diversos domínios que configuram a exposição digital das empresas, nomeadamente a ligação à Internet, a presença digital, as compras e vendas *online*, a interconexão automática com clientes e fornecedores, a adoção de sistemas de alojamento remoto e a integração de outros sistemas de operação automática ou autónoma, as empresas portuguesas estão, ainda, atrás das suas congéneres europeias. Embora esta situação possa afetar negativamente a competitividade do tecido empresarial português, do ponto de vista da cibersegurança poderá ser aproveitada para melhorar os níveis de segurança informática, reduzindo assim o número de incidentes e as suas consequências operacionais e financeiras.

Para a maioria das PMEs portuguesas a principal barreira à implementação de medidas para melhorar os níveis de cibersegurança é o seu custo. Outros impedimentos apontados são a escassa cultura de cibersegurança dos colaboradores, a falta de pessoal adequado ou qualificado e o desconhecimento das medidas a adotar. As PMEs do país enfrentam poucos incidentes de segurança e, genericamente, são pouco sofisticados e implicam custos relativamente baixos. Em geral, as PMEs dispõem de medidas de proteção contra esse tipo de incidentes, mas tendem a ser relativamente simples, e apenas uma proporção marginal possui seguros contra riscos cibernéticos.

Considerando apenas empresas cujo volume de negócios procede, em grande medida, da prestação de serviços de cibersegurança, este sector em Portugal é constituído por 144 empresas, que empregam aproximadamente 1.300 trabalhadores e têm um volume de negócios conjunto de cerca de 130 milhões de euros. Para além das empresas prestadoras de serviços de segurança informática, existe um número considerável, embora insuficiente, de profissionais de cibersegurança. Trata-se de profissionais relativamente jovens, experientes, qualificados e comparativamente bem remunerados.

As principais recomendações do estudo são as seguintes:

A nível macro, recomenda-se:

- Potenciar a arquitetura institucional da cibersegurança em Portugal, melhorando os sistemas de comunicação com as empresas, os sistemas de reporte de incidentes e ciberataques e, em geral, os mecanismos de integração entre os diversos integrantes do ecossistema de cibersegurança no país;
- No âmbito dos desenvolvimentos na União Europeia, manter atualizado o quadro regulamentar e institucional do país em matéria de cibersegurança, garantindo a sua adaptabilidade num contexto extremamente mutante;
- Promover a notabilização da problemática da cibersegurança e dos impactos dos incidentes cibernéticos e dos ciberataques, através de práticas de *lobby* em determinados âmbitos e de campanhas de visibilização e sensibilização destinadas a públicos com diferentes níveis de exposição e risco;
- Acompanhar os desenvolvimentos e iniciativas da União Europeia no âmbito da cibersegurança e promover a participação ativa de parceiros portugueses nas mesmas – administrações, organismos públicos, reguladores, universidades, institutos, o exército, empresas, associações ou parceiras público-privadas, entre outras;
- Participar nos programas, projetos e iniciativas promovidos pelas entidades internacionais de que Portugal é membro, com a finalidade de manter um quadro institucional e legal atualizado e uma elevada capacidade de resposta face aos desafios atuais e emergentes em matéria de cibersegurança;
- Desenvolver iniciativas para aumentar os níveis de proteção de infraestruturas e entidades críticas e de cadeias de valor estratégicas à escala nacional ou internacional, com forte presença em território português;
- Dar continuidade à política de acompanhamento das tendências, riscos, incidentes, práticas, políticas e regulação de cibersegurança, para melhorar a tomada de decisões nesta matéria em diversos âmbitos. Neste contexto, os contributos do CNCS, em Portugal, e da ENISA, a nível europeu, afiguram-se fundamentais;

- Monitorizar as possibilidades de financiamento, para reforçar a cibersegurança nas empresas, que oferecem e vão continuar a oferecer os programas de financiamento europeu, nomeadamente em matéria de inovação, criação de capacidades, formação, capacitação e reciclagem de recursos humanos e adquisição de sistemas de proteção, entre outros;
- Reforçar a atratividade dos programas de formação em TIC no ensino superior, através de campanhas de diversa natureza, destinadas especialmente às jovens. O aumento da procura pelos profissionais de TIC, sem que se verifique um aumento da oferta de graduados nessas áreas, poderá dar origem a escassez e provocar aumentos salariais, e consequentemente, dificultar a contratação desses profissionais pelas empresas financeiramente mais frágeis;
- Aumentar a oferta de programas de formação superior na área da cibersegurança, especialmente ao nível de licenciatura, criando especializações na área da segurança cibernética. Conviria reforçar também a oferta de cursos TeSP, de nível secundário não terciário, dedicados integral ou parcialmente à cibersegurança, para formar profissionais que possam dar resposta a necessidades menos sofisticadas nas empresas;
- Realizar campanhas de sensibilização, junto das empresas, sobre a problemática da cibersegurança, o impacto de incidentes e ataques, as formas de proteção e as políticas e protocolos para melhorar os níveis de proteção, gerir incidentes de segurança e ciberataques e atuar nas fases posteriores aos mesmos.

Dados os condicionantes ao investimento em cibersegurança por parte das empresas, do ponto de vista regulatório deve/m:

- Promover-se a adoção de medidas preventivas e de boas práticas em matéria de segurança cibernética, nomeadamente do Quadro Nacional de Referência para a Cibersegurança (QNRCS);
- Assegurar-se o reporte de incidentes de segurança e de ciberataques, nomeadamente dos mais relevantes, e divulgar informação de interesse geral sobre os mesmos;
- Impulsionar-se, tal como pretende o CNCS, a criação de Centros de Análise e Partilha de Informação (ISAC) sectoriais, especialmente no âmbito dos sectores mais críticos e sensíveis, que para além de partilhar e analisar informação, permitam reforçar a confiança e desenvolver competências e capacidades;
- Desenvolver-se políticas de certificação das empresas e dos profissionais, para garantir protocolos e procedimentos e informar sobre os níveis de proteção das empresas e a qualidade dos prestadores de serviços, sejam eles empresas ou profissionais;
- Impulsionar-se o desenvolvimento do mercado de seguros cibernéticos e incentivar-se a contratação destas coberturas por parte das empresas.

Dadas as tendências em termos de exposição e de evolução dos mercados, a nível empresarial convém:

- Reforçar a cultura de cibersegurança, generalizar medidas de cibersegurança e formalizar protocolos de cibersegurança;
- Melhorar os processos de gestão da identidade e de autenticação para aceder aos sistemas empresariais;
- Fortalecer os mecanismos de proteção, deteção e resposta dos sistemas empresariais e, em especial, dos baseados em soluções *cloud*;
- Em entidades com elevados níveis de exposição e risco de perda, intensificar o recurso a técnicas avançadas de cifra e ao *blockchain* a fim de garantir a integridade dos dados e reforçar a segurança;
- Aumentar a segurança nas cadeias de fornecimento e nos sistemas logísticos;
- Em entidades com elevados níveis de exposição e risco de perda, incorporar novas formas de proteção, identificação e resposta baseadas em IA, *Machine Learning* e outras soluções automatizadas;
- Adotar tecnologias e controlos para gerir ameaças crescentes (ex. o *ransomware* ou a engenharia social);
- Melhorar a adaptação às novas regulações em matéria de segurança, privacidade de dados pessoais e comportamento das pessoas no ciberespaço, bem como disponibilizar meios humanos para o efeito;
- Atendendo à sofisticação crescente das ameaças e dos ataques, migrar progressivamente para um modelo baseado na externalização total ou parcial dos serviços de cibersegurança, designadamente entre as empresas de menor dimensão.

No futuro, os estudos sobre a dimensão económica da cibersegurança em Portugal deveriam abordar assuntos como a caracterização das entidades e infraestruturas críticas e das grandes empresas, assim como as suas práticas e protocolos de cibersegurança, e a identificação dos principais prestadores de serviços de cibersegurança no país e a análise do seu posicionamento e estratégias a médio prazo. Na dimensão macro teria interesse mensurar o contributo da cibersegurança para o crescimento económico em Portugal, e na sectorial avaliar os défices e potencialidades do país para reforçar o seu ecossistema privado de cibersegurança e atrair investimento para o seu desenvolvimento futuro.

METODOLOGIA

METODOLOGIA CAPÍTULO IV

DELIMITAÇÃO DO SECTOR DE CIBERSEGURANÇA EM PORTUGAL

IV.1 FONTE DE DADOS

ORBIS EUROPE. Base de dados produzida pela empresa Bureau van Dijk, disponível em https://orbiseurope.bvdinfo.com/. Contém informação financeira de mais de 75 milhões de empresas localizadas na Europa. Dados recolhidos no dia 13-07-2021.

IV.2 SELEÇÃO DAS EMPRESAS

1º PASSO

Foram selecionadas todas as empresas da classe CAE Rev3:

- 6201 – Atividades de programação informática
- 6202 – Atividades de consultoria em informática
- 6203 – Gestão e exploração de equipamento informático
- 6209 – Outras atividades relacionadas com as tecnologias da informação e informática
- 6311 – Atividades de processamento de dados, domiciliação de informação e atividades relacionadas
- 6312 – Portais Web
- 6399 – Outras atividades dos serviços de informação, n.e.

O número total de empresas selecionadas foi de 6.835.

2º PASSO

Pesquisa textual dos termos "segurança", "incidente", "ataque", "cibersegurança" na descrição do objeto social da empresa (variável "Trade description in original") e do termo "security" na descrição do produto ou serviço (variável "Products services").

Foram selecionadas as empresas que incluem os termos pesquisados.

3º PASSO

Verificação "manual" das empresas selecionadas. Constituição de dois grupos de empresas: (1) Nuclear – empresas em que a venda de produtos ou de serviços associados à cibersegurança é explícita no seu objeto social; (2) Potencial – restantes empresas da Divisão 62 Consultoria e programação informática e atividades relacionadas e Divisão 63 Atividades dos serviços de informação, que não indicando explicitamente os termos acima referidos, assume-se que potencialmente poderão fornecer produtos ou serviços de cibersegurança.

4º PASSO

Foram excluídas as empresas com volume de negócios nulo ou com um número de trabalhadores igual a zero no ano de 2019. O número final de empresas analisadas é de 5.717, sendo 144 do grupo "Nuclear" e 5.573 do grupo "Potencial".

METODOLOGIA CAPÍTULO V

INQUÉRITO ÀS PEQUENAS E MÉDIAS EMPRESAS PORTUGUESAS SOBRE CIBERSEGURANÇA

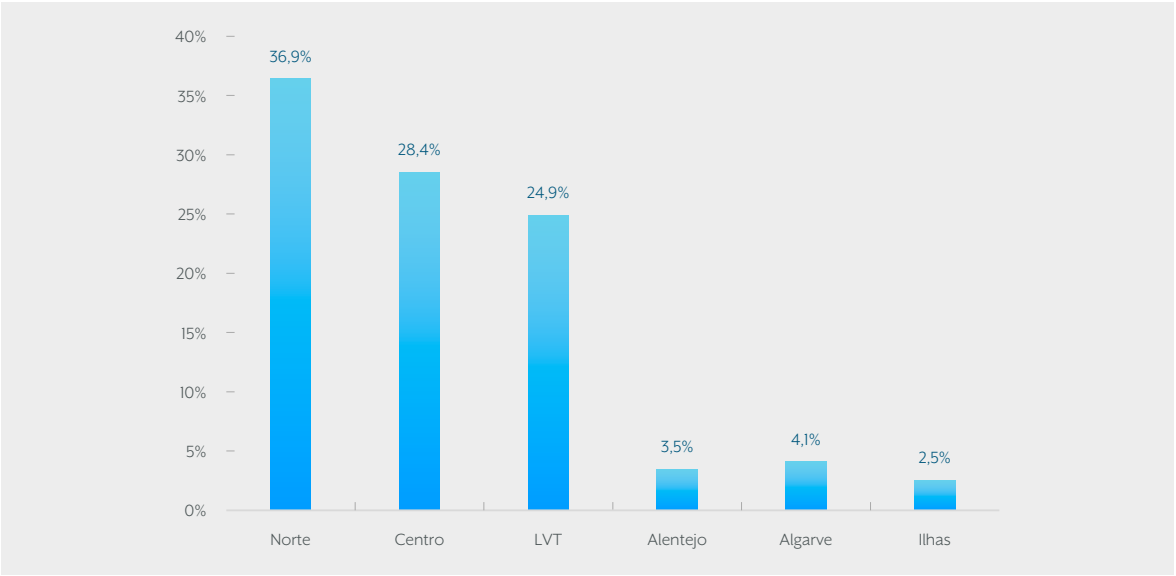
V.1 PROCEDIMENTO

O inquérito às PMEs foi promovido pelo CNCS e contou com o apoio do IAPMEI. O questionário foi desenhado pela equipa da Universidade do Minho e foi revisto pelo CNCS e pelo IAPMEI. Esta entidade enviou um *e-mail* com um *link* para o questionário, alojado numa plataforma do CNCS. O inquérito permaneceu aberto durante três semanas aproximadamente, entre setembro e outubro de 2021.

V.2 CARACTERIZAÇÃO DA AMOSTRA DE EMPRESAS PARTICIPANTES

Foram recolhidas 641 respostas válidas de empresas de todo o país (Figura M-V.1). A maioria das empresas localizam-se nas NUT II Norte, Centro e Lisboa e Vale do Tejo (LVT).

Figura M-V.1 – Localização das empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Nota 1

Para efeitos de análise, as respostas foram categorizadas em função dos sectores a que pertencem as empresas.[78] Dado o reduzido número de empresas da indústria extrativa, as respostas deste sector juntaram-se às da indústria transformadora. As empresas do sector da construção mantiveram-se separadas.

O sector serviços foi dividido em três subsectores, tendo em atenção a existência de afinidades que podem traduzir-se em riscos de cibersegurança semelhantes e em respostas e comportamentos similares. Desta forma, as empresas agruparam-se da seguinte forma: comércio, restauração e alojamento;[79] serviços de reduzido valor acrescentado (v.a.); e, serviços de elevado valor acrescentado (v.a.).

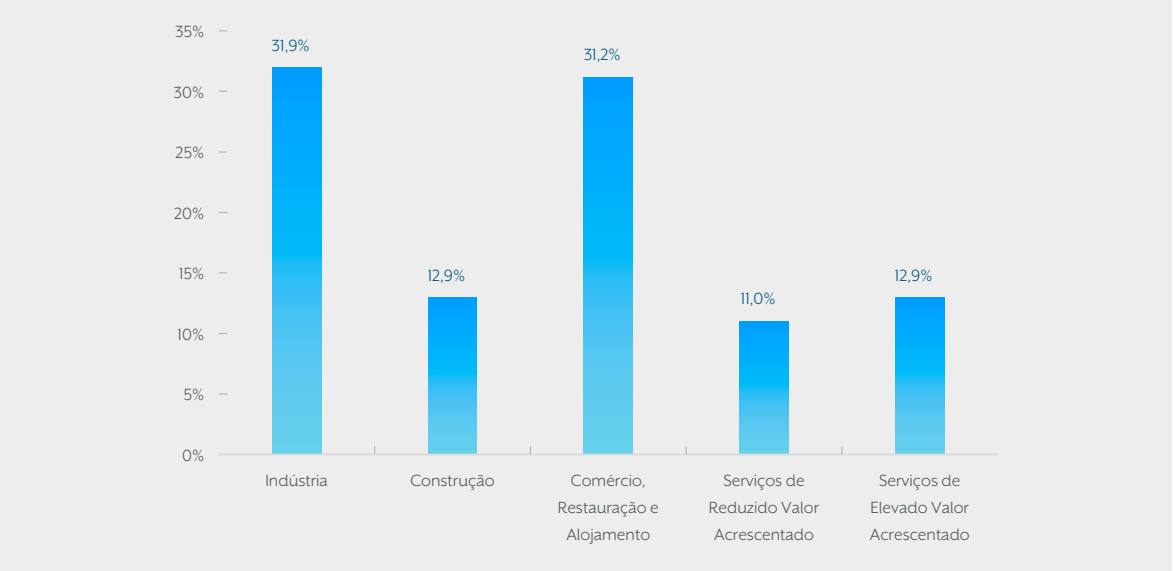
Os serviços de reduzido valor acrescentado incluem: transportes e armazenagem; atividades imobiliárias; atividades administrativas e dos serviços de apoio; atividades artísticas, de espetáculos, desportivas e recreativas; e, outras atividades de serviços. Os serviços de elevado valor acrescentado agrupam: atividades de informação e de comunicação; atividades financeiras e de seguros; atividades de consultoria, científicas, técnicas e similares; administração pública e defesa; educação; e outras atividades de serviços.

Na Figura M-V.2. é apresentada a divisão sectorial da amostra. Mais de seis em cada dez empresas pertencem à indústria e ao comércio, restauração e alojamento.

78. Na análise sectorial foram retiradas as respostas das cinco empresas do sector primário participantes, por não serem representativas do sector e a fim de evitar enviesamentos na interpretação dos resultados.

79. Também denominadas no texto Comércio e afins

Figura M-V.2 – Distribuição sectorial das empresas, Portugal, % de empresas



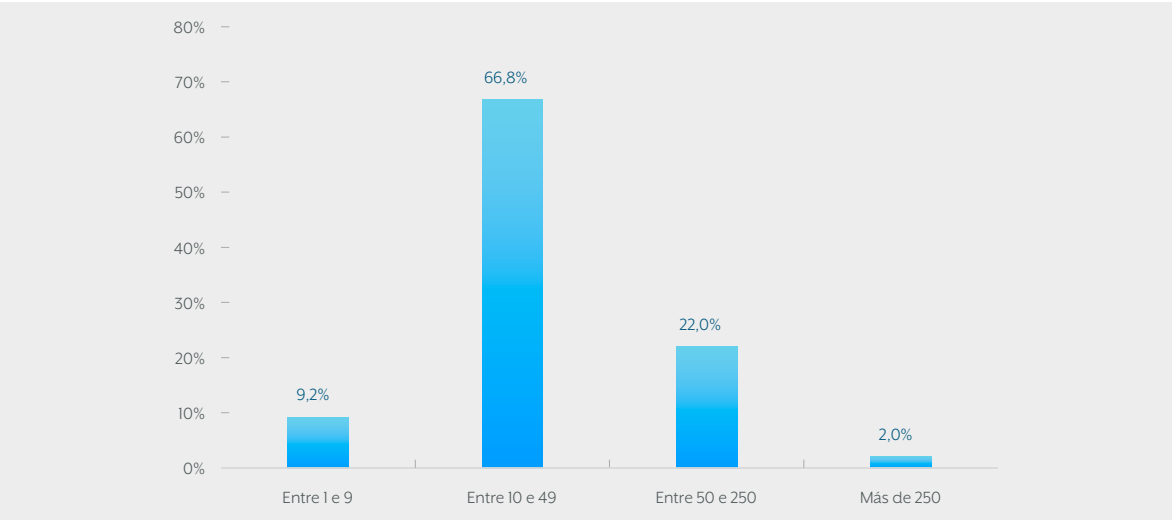
Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Quase 90% das empresas participantes são PMEs (Figura M-V.3). Dois terços das respondentes são pequenas empresas (10 a 49 trabalhadores) e pouco mais de um quinto médias empresas (50 a 250 trabalhadores). As microempresas e especialmente as grandes empresas têm escassa representatividade na amostra.

Nota 2

Dada a reduzida proporção de empresas de grande dimensão existentes na amostra e a fim de evitar enviesamentos nos resultados, para efeitos de análise foram retiradas de amostra, uma vez que as suas políticas, práticas e protocolos no âmbito digital e em matéria de cibersegurança são bastante diferentes dos das empresas de menor dimensão. Após a análise detalhada das respostas das microempresas, verificou-se que uma parte considerável das questões não foram respondidas, por falta de aplicação ou desconhecimento. Este grupo de empresas foi mantido na amostra para efeitos de apresentação de resultados, mas não foi realizada uma análise separada para este grupo em concreto.

Figura M-V.3 – Empresas por número de trabalhadores, Portugal, % de empresas



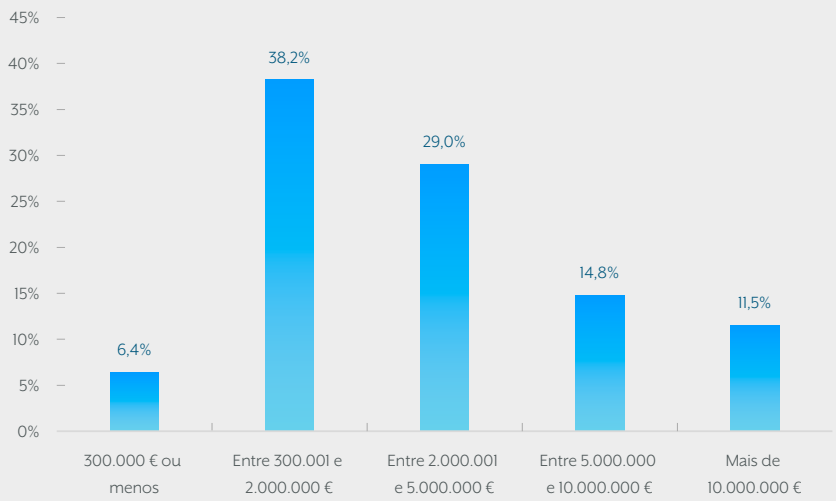
Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Quase quatro em cada dez empresas participantes faturam entre 300.000 e dois milhões de euros e três em cada dez entre dois e cinco milhões de euros (Figura M-V.4). Aproximadamente um quarto das empresas tem um volume de negócios superior a cinco milhões de euros.

Entre as pequenas empresas, metade possui um volume de negócios compreendido entre 300.000 e dois milhões de euros e um terço entre dois e cinco milhões de euros. Aproximadamente uma em cada dez empresas fatura entre cinco e dez milhões de euros. No caso das médias empresas, pouco mais de um terço tem um volume de faturação situado entre cinco e dez milhões de euros e uma proporção similar superior a dez milhões. Aproximadamente uma em cada cinco empresas médias fatura entre dois e cinco milhões de euros e à volta de 7% vende menos de dois milhões de euros.

Por sectores, as empresas com maiores volumes de faturação são as do sector industrial. Um terço das empresas industriais fatura mais de cinco milhões de euros. No sector do comércio, restauração e alojamento, aproximadamente um quarto das empresas fatura acima desse valor. Nos restantes sectores, aproximadamente uma em cada cinco empresas tem um volume de negócios superior a cinco milhões de euros. No sector dos serviços de elevado v.a., o peso das empresas que faturam menos de 300.000 euros é de cerca de 30%, muito superior ao de qualquer outro dos sectores considerados.

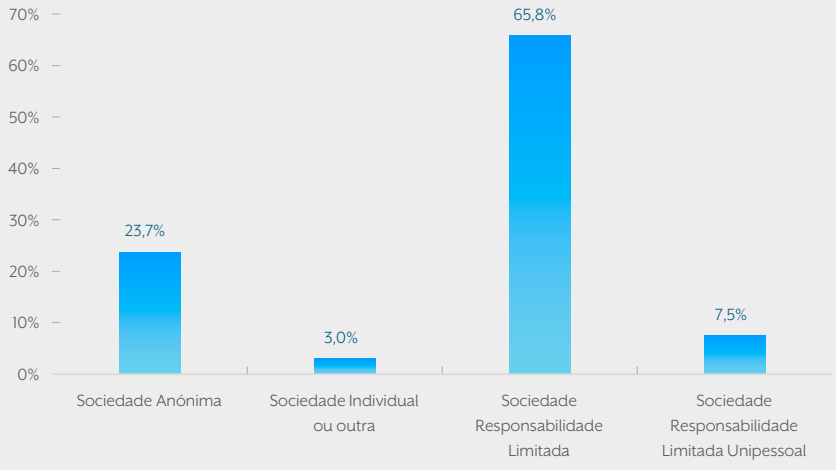
Figura M-V.4 – Empresas por volume de negócios, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

Quase dois terços das empresas participantes são sociedades de responsabilidade limitada e quase um quarto são sociedades anónimas (Figura M-V.5). Entre as pequenas empresas, três quartos são sociedades de responsabilidade limitada e um sexto sociedades anónimas.

Figura M-V.5 – Forma jurídica da empresa, para todas as empresas, Portugal, % de empresas



Fonte: Inquérito às empresas portuguesas sobre Cibersegurança.

A sociedade anónima é a forma jurídica dominante entre as médias empresas, dado que uma em cada duas possui esta figura societária. Neste grupo, as sociedades de responsabilidade limitada representam mais de dois quintos do total.

As sociedades de responsabilidade limitada unipessoal representam em torno dos 7% em todos os segmentos considerados. Outras formas jurídicas, nomeadamente os empresários em nome individual, têm um peso marginal, que tende a reduzir-se à medida que aumenta o tamanho da empresa.

As sociedades anónimas têm um peso significativo no sector industrial (quase um terço) e nos sectores de serviços de elevado v.a. (pouco mais de um quinto). Curiosamente é nesses dois sectores onde as sociedades de responsabilidade limitada têm menor ponderação (por volta de seis em cada dez empresas, em ambos os casos). Nos restantes sectores, sete em cada dez empresas têm essa natureza jurídica. As sociedades de responsabilidade limitada individual têm alguma expressão no sector da construção e no de serviços de elevado v.a. (entre 10-15%, em ambos casos). Nos restantes sectores a sua representatividade é marginal.

V.3 ABORDAGEM DE APRESENTAÇÃO

Na apresentação de resultados, atendendo ao número de respostas obtidas e à qualidade das mesmas, entende-se que, em certos casos, é oportuna a realização de uma análise separada para as pequenas e para as médias empresas, dado que, em algumas dimensões, foram identificados aspetos onde a abordagem, as políticas e os comportamentos diferem consideravelmente. Assim sendo, a análise dos resultados do inquérito é, na maioria dos casos, apresentada para três tipologias de empresas: todas as empresas (micro, pequenas e médias), pequenas empresas e médias empresas. Uma aproximação similar foi adotada ao nível sectorial, embora neste caso limitou-se a apresentação gráfica dos resultados, para evitar a excessiva proliferação de figuras. Quer no âmbito da dimensão empresarial, quer no âmbito setorial, quando não existam diferenças assinaláveis, apenas são apresentados os resultados em termos agregados.


Bitcoin
BTC
Ethereum
ETH
Tether
USDT
Dogecoin
DOGE
Cardano
ADA
Polkadot
DOT
Ripple
XRP
Litecoin
LTC

Centro Nacional de Cibersegurança
Rua da Junqueira, 69 | 1300-342 Lisboa
cncs@cncs.gov.pt
(+351) 210 497 400