CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Observatório de Cibersegurança

DEZEMBRO 2022

RELATÓRIO CIBERSEGURANÇA EM PORTUGAL

SOCIEDADE 2022

4ª EDIÇÃO

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

FICHA TÉCNICA

Autoria e edição: Centro Nacional de Cibersegurança
Design: Nova Agência

www.cncs.gov.pt

ÍNDICE

“A UTILIZAÇÃO DA VULNERABILIDADE HUMANA COMO VETOR DE ATAQUE NO CIBERESPAÇO CONTINUA A SER MUITO FREQUENTE”

A. SUMÁRIO EXECUTIVO

A dimensão comportamental da cibersegurança tem mantido a sua relevância, apesar do desenvolvimento tecnológico e das novas soluções digitais de segurança. Os dados mostram que a utilização da vulnerabilidade humana como vetor de ataque no ciberespaço continua a ser muito frequente, conduzindo, por vezes, a grandes impactos (CNCS, 2022a). Por isso, o *Relatório Cibersegurança em Portugal, tema Sociedade*, enquanto o documento do Observatório de Cibersegurança dedicado às atitudes, comportamentos, sensibilização e educação em cibersegurança, continua a merecer uma periodicidade anual na sua publicação, de modo a acompanhar e medir as transformações nesta matéria. A análise, tal como em anos anteriores, sistematiza a informação disponível sobre este assunto e produz aquela que se identifica como estando em falta, apresentando uma visão integrada.

Este relatório divide-se em quatro áreas temáticas relativas a Portugal, com particular incidência em 2021 (mas também com alguns dados de 2022):

1. Ambiente sociotécnico, em que se analisa a evolução dos usos da Internet e serviços digitais;
2. Pesquisas *online*, onde se apresentam dados sobre o interesse pela pesquisa da palavra "cibersegurança";
3. Atitudes e comportamentos, momento em que se expõem os indicadores disponíveis sobre as perceções e as boas práticas relativos à cibersegurança em indivíduos e organizações;
4. Sensibilização e educação, etapa dedicada à evolução das ações de sensibilização em ciber-higiene e aos cursos especializados em cibersegurança e segurança de informação.

Procura-se ainda verificar, ao longo do documento e num capítulo específico, se os indicadores analisados permitem correlações com as linhas de ação da Estratégia Nacional de Segurança do Ciberespaço 2019- 2023 (ENSC), no sentido de ponderar eventuais impactos desta na sociedade portuguesa e necessidades de reajustes na sua execução ou orientações para uma nova estratégia.

ANÁLISE GLOBAL

Considere-se de seguida, para uma análise global sumária, as principais tendências e destaques que resultam deste estudo.

TENDÊNCIAS

AMBIENTE SOCIOTÉCNICO E PESQUISAS *ONLINE*

Verifica-se, em 2021, uma tendência, que já se fazia sentir em 2020, de aumento dos usos da Internet e de alguns serviços críticos para a cibersegurança, como o *email*, o telefone e videochamadas *online*, as mensagens instantâneas, o banco *online* e as compras *online*.

> UMA MAIOR UTILIZAÇÃO DESTAS PLATAFORMAS SIGNIFICA UMA MAIOR EXPOSIÇÃO AOS RISCOS

Ameaças muito frequentes como o *phishing, o vishing, o smishing*, o comprometimento de contas e a burla *online* utilizam estes serviços como superfícies de ataque. Uma maior utilização destas plataformas significa uma maior exposição aos riscos, logo, uma maior necessidade de cuidados.

O termo "cibersegurança" passou a ser mais pesquisado *online* em Portugal a partir de 2020, comparando com 2019, verificando-se uma ligeira descida em 2021 e um aumento significativo no primeiro semestre de 2022. Acontecimentos como a pandemia e ataques muito relevantes a organizações portuguesas podem ter contribuído para este crescimento.

ATITUDES E COMPORTAMENTOS

Verifica-se uma tendência positiva no que se refere ao conhecimento e práticas relativos à gestão dos dados pessoais *online* por parte dos indivíduos. Existe ainda uma discrepância entre perceção e realidade relativamente às compras *online*: a ideia de que a segurança e a privacidade são problemas é muito maior entre os indivíduos que percecionam aí uma barreira às compras *online*, ao ponto de não as realizarem, comparando com os problemas de fraude efetivamente identificados entre os que fazem esse tipo de compras.

As pequenas e médias empresas (PME) portuguesas reconhecem mais que sofrem cibercrimes e revelam mais preocupações quanto aos riscos de os virem a sofrer do que a média da União Europeia (UE), mas também reportam mais os incidentes às autoridades do que a média da UE.

No âmbito da Administração Pública, são notórias algumas tendências negativas: existem menos estratégias para a segurança de informação definidas e uma maior necessidade de reforço das competências em segurança das Tecnologias de Informação e Comunicação (TIC). Mais positivos são os dados que mostram aumentos na aplicação de medidas de segurança das TIC e na disponibilização de recomendações de boas práticas nestes organismos.

SENSIBILIZAÇÃO E EDUCAÇÃO

Existe uma grande predominância, em termos de tipologia de ações de sensibilização em cibersegurança, realizadas por organizações com a missão de efetuar essas ações junto de públicos externos, das sessões presenciais ou *online* comparativamente a outros tipos de ações. Todavia, os cursos *online* mostram uma maior eficácia em termos do número de pessoas alcançadas, o que não significa que tenham melhores efeitos no comportamento. A maioria destas organizações não avalia o impacto das suas ações de sensibilização no comportamento do público-alvo, o qual é sobretudo adulto e sem predomínio de sexo. Os temas mais comuns são os relacionados com boas práticas genéricas de ciber-higiene.

Poucas PME portuguesas realizam ações de sensibilização aos seus funcionários no âmbito da cibersegurança. A Administração Pública efetua essas ações com maior frequência, mas sobretudo de forma voluntária, poucas são obrigatórias. Não obstante, a percentagem deste tipo de ações na Administração Pública está a aumentar.

Verifica-se um crescimento no número de cursos superiores de cibersegurança e segurança de informação, nomeadamente cursos de Técnico Superior Profissional (TESP), e também de alunos inscritos. Há, por outro lado, um decréscimo no número de alunos diplomados. A proporção de mulheres inscritas e diplomadas continua a ser reduzida e apresenta um valor abaixo da proporção de mulheres diplomadas em cursos de TIC em Portugal.

CENÁRIOS DE AMEAÇAS E O FATOR HUMANO

Os anos de 2020 e 2021 foram particularmente marcados pela pandemia da Covid-19 e pelas consequências sociais e económicas da mesma. Como foi verificado em termos de ameaças nos relatórios do Observatório de Cibersegurança dedicados aos *Riscos e Conflitos* 2021 e 2022 (CNCS, 2021a e 2022a), neste período verificou-se um aumento no número de incidentes e cibercrimes. Contudo, a mitigação progressiva da pandemia e o surgimento de uma guerra na Ucrânia fizeram emergir novos fatores de ameaça.

O contexto de pandemia favoreceu as burlas *online*, o comprometimento de sistemas próprios do trabalho remoto (RDP, VPN) e o *phishing*, verificando-se como temáticas dominantes de *phishing* as ligadas à banca, aos transportes e logística e à captura de credenciais de *email*. Por outro lado, com o emergir da guerra na Ucrânia, já em 2022, surgem com um reforço na sua relevância a ciberespionagem, o comprometimento de cadeias de fornecimento, o DDoS e o *phishing* dirigido a pessoas específicas (*spear phishing*), entre outros, com tendência para afetar a Administração Pública e os operadores de serviços essenciais. Em ambos os cenários, algumas ameaças são constantes, como o *ransomware*, por exemplo. Em 2021, em particular, persistiram como ameaças importantes o *phishing/smishing/vishing*, o *ransomware*, a fraude/burla *online*, o comprometimento de contas e a exploração de vulnerabilidades (CNCS, 2022a). Em qualquer dos casos, as fragilidades do fator humano são recorrentemente exploradas como vetores de ataque.

As atitudes, os comportamentos, a sensibilização e a educação são tópicos fundamentais para promover o reforço do fator humano. Considerando as principais conclusões deste relatório e as ameaças mais relevantes de 2021 (ver quadro 1), verifica-se a existência de algumas circunstâncias que têm um contributo negativo para a mitigação das ameaças: o aumento dos usos da Internet e serviços digitais; a diminuição do número de estratégias de segurança de informação e a falta de profissionais da área na Administração Pública; a existência de poucas ações de sensibilização nas PME e, as que se realizam na Administração Pública, serem sobretudo voluntárias; a diminuição do número de diplomados em cursos especializados; e os desequilíbrios sociodemográficos relativamente aos conhecimentos, práticas e ações de sensibilização em cibersegurança. Com um contributo em geral positivo, encontram-se as seguintes situações: a razoável gestão dos dados pessoais *online* por parte dos indivíduos e a sua preocupação com as compras *online* (embora uma preocupação que conduza ao não uso nem sempre seja positiva); a elevada preocupação das PME com os riscos de cibercrime e a significativa tendência para reportarem incidentes; os aumentos na aplicação de medidas de segurança das TIC e na distribuição de recomendações deste âmbito na Administração Pública; o alcance generalizado das ações de sensibilização em cibersegurança em termos temáticos e de público-alvo; e o crescimento do número de cursos e alunos especializados em cibersegurança e segurança de informação.

Algumas ameaças afetam alvos e exigem competências e práticas mais individuais, como a fraude/burla *online*; outras, mais organizacionais, como o *ransomware*; outras ainda, têm um caráter mais técnico, como a exploração de vulnerabilidades; enquanto o *phishing*, por exemplo, depende muito do fator humano. Estas diferenças interferem na relevância de cada boa prática em relação a cada ameaça.

Quadro 1

RELAÇÃO ENTRE RESULTADOS DESTE RELATÓRIO E PRINCIPAIS AMEAÇAS AO CIBERESPAÇO DE INTERESSE NACIONAL, EM 2021

Resultados *Sociedade 2022* / Ameaças *Riscos e Conflitos* 2022 (CNCS, 2022)	Phishing Smishing Vishing	Ransomware	Fraude Burla *online*	Comprometimento de contas	Exploração de vulnerabilidades
Maior risco fruto de aumento dos usos da Internet e serviços digitais					
Melhor gestão dos dados pessoais e elevada preocupação com compras *online*					
Elevada preocupação das PME com riscos e elevado reporte de incidentes					
Menos estratégias de segurança de informação na Administração Pública					
Elevada necessidade de competências de segurança das TIC na Administração Pública					
Mais medidas aplicadas e recomendações distribuídas na Administração Pública					
Alcance genérico das ações de sensibilização em termos temáticos e de público-alvo					
Poucas ações de sensibilização nas PME e poucas obrigatórias na Administração Pública					
Mais cursos especializados e mais alunos a frequentar os mesmos					
Menos diplomados em cursos especializados					
Desequilíbrios sociodemográficos nos conhecimentos, práticas e sensibilização					

 Contributo negativo para a mitigação da ameaça
 Contributo positivo para a mitigação da ameaça
 Contributo não decisivo para a mitigação da ameaça

ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO 2019-2023

No âmbito do acompanhamento da ENSC, é possível identificar cinco grandes domínios com os quais os resultados deste Relatório se relacionam e em que é possível identificar aspetos positivos e negativos, em particular no que diz respeito ao Eixo 2 - Prevenção, educação e sensibilização e, em parte, ao Eixo 1 - Estrutura de segurança do ciberespaço.

1. Relativamente à sensibilização do cidadão em geral, embora existam dados positivos quanto a alguns comportamentos, as ações de sensibilização nas organizações são insuficientes ou apenas voluntárias. As ações de sensibilização que se dirigem ao cidadão em geral têm um peso elevado de temas genéricos de cibersegurança e tendem a não se restringir a um público-alvo específico, aspeto positivo no que se refere ao alcance.
2. No que diz respeito à sensibilização de grupos específicos, persistem desequilíbrios sociodemográficos, em que os adultos mais velhos e as pessoas com menos formação têm menos conhecimentos e cuidados de ciber-higiene. As ações de sensibilização tendem a não focar suficientemente grupos específicos, nomeadamente adultos mais velhos.
3. Quanto ao objetivo de introduzir o tema da cibersegurança na educação formal, o aumento de cursos especializados e de alunos é um dado positivo, embora haja menos diplomados.
4. Quanto à necessidade de qualificação de especialistas, verifica-se que esta necessidade persiste elevada na Administração Pública em particular.
5. Por fim, considerando as linhas de ação que promovem a colaboração entre entidades na reação a incidentes, a tendência das PME portuguesas para reportarem incidentes é positiva.

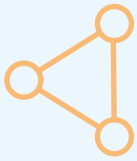
DESTAQUES

AMBIENTE SOCIOTÉCNICO E PESQUISAS *ONLINE* SOBRE "CIBERSEGURANÇA" EM PORTUGAL

Verificou-se um aumento do uso da Internet em 4 pp, de 78% dos indivíduos em 2020 para 82% em 2021. Ainda assim, este valor é menor em 7 pp do que a média da UE (Eurostat).

Há mais indivíduos a usar alguns serviços *online* críticos em 2021 do que em 2020: o *email* (88% - mais 1 pp e 3 pp acima da média da UE); o telefone e videochamadas *online* (80% - mais 10 pp e 7 pp acima da média da UE); as mensagens instantâneas (91% - mais 1 pp e 12 pp acima da média da UE); banco *online* (64% - mais 4 pp e 2 pp abaixo da média da UE); e as compras *online* (40% - mais 5 pp e 17 pp abaixo da média da UE) (Eurostat).

As redes sociais, embora não sejam mais usadas em 2021 do que em 2020, mantêm-se a ser usadas por 80% dos indivíduos em Portugal, mais 16 pp do que a média da UE, que é de 64% (Eurostat).



As pesquisas *online* pela palavra "cibersegurança" aumentaram de forma significativa em 2020, diminuindo ligeiramente em 2021. Em 2022, voltaram a aumentar no primeiro semestre de forma muito significativa (Google Trends).

Os distritos de Lisboa, Setúbal e Coimbra são as regiões com mais interesse pela pesquisa da palavra "cibersegurança" a nível nacional, proporcionalmente em relação à dimensão de cada uma destas regiões (Google Trends).

Os tópicos paralelos (não sinónimos de "cibersegurança") mais relevantes nestas pesquisas são "CNCS" e os ligados ao tema da educação, como "disciplina" e "mestrado" (Google Trends).

ATITUDES E COMPORTAMENTOS EM PORTUGAL

Verifica-se uma tendência positiva, em 2021, relativamente ao conhecimento que os indivíduos possuem sobre os *cookies*, com 63% de respostas positivas, uma melhoria de 4 pp comparando com 2020. Ainda assim, 9 pp abaixo da média da UE (Eurostat).

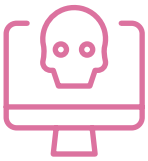
Em 2021, existem mais cuidados com a gestão dos dados pessoais *online* por parte dos indivíduos do que em 2020 (71% utiliza pelo menos um método de gestão - mais 3 pp), valor acima da média da UE (em 6 pp) (Eurostat).

As pessoas mais velhas e as que têm formação básica demonstraram, em 2021, ter menos cuidados com a privacidade e a proteção de dados pessoais *online* do que os jovens e do que as pessoas com formação superior. No entanto, as pessoas com formação básica percecionaram mais barreiras às compras *online* devido a preocupações de segurança do que as que têm formação superior (Eurostat).

Os indivíduos, em 2021, percecionaram como barreiras às compras *online* as preocupações de segurança e privacidade em maior volume do que a média da UE (27% em Portugal e 6% na média da UE). Contudo, apenas 1% dos que compraram *online* encontraram problemas de fraude (em Portugal e na média da UE) (Eurostat).

Há menos inquiridos com funções de topo nas PME portuguesas, em 2021, a sentirem-se bem informados sobre os riscos de cibercrime do que a média da UE (67% - menos 4 pp do que a média da UE) (Eurobarómetro).

As PME portuguesas, em 2021, mostram-se mais preocupadas com os riscos *online* do que a média da UE (e. g., 55% estão preocupadas com o *hacking* a contas bancárias *online*, enquanto a média da UE é de 32%) (Eurobarómetro).



Há mais PME portuguesas, em 2021, a admitirem ter sofrido pelo menos um cibercrime nos últimos 12 meses (48%) do que a média da UE (28%) (Eurobarómetro).

Em 2021, o impacto mais sentido pelas PME portuguesas como resultado do incidente mais grave foi a impossibilidade de uso de recursos ou serviços (para 32%). Na média da UE foi o tempo despendido a responder ao incidente (35%) (Eurobarómetro).

As PME portuguesas, em 2021, reportaram mais incidentes do que a média da UE (81% em Portugal e 54% na média da UE). A entidade a quem mais reportaram foi a polícia (24%) e, quando não reportaram, a razão mais apresentada foi considerarem o caso demasiado trivial (27%) (Eurobarómetro).

A percentagem de organismos da Administração Pública com uma estratégia para a segurança de informação definida diminuiu em 2021, comparando com 2020, em 2 pp, fixando-se em 59% (DGEEC).

Em 2021, há mais organismos da Administração Pública a aplicarem medidas de segurança das TIC, com particular destaque para a Administração Regional da Madeira (DGEEC).

Existem mais organismos da Administração Pública, em 2021, a indicarem ter elevada necessidade de reforço de competências em segurança das TIC, fixando-se em 69%, mais 7 pp do que no ano anterior (DGEEC).

Nas Câmaras Municipais do Norte do país, em 2021, verifica-se alguma correlação entre a existência de uma elevada necessidade de reforço de competências em segurança das TIC e a ausência de estratégias para a segurança de informação definidas. Na Área Metropolitana de Lisboa essa correlação não existe, indiciando-se uma correlação inversa (DGEEC).

Predomina pessoal do próprio organismo, na Administração Pública, na realização de atividades relacionadas com a segurança das TIC, em 2021 (entre 40% e 51%) (DGEEC).

O número de entidades da Administração Pública com recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC aumentou 2 pp em 2021, verificando-se em 47% das mesmas (DGEEC).

Há menos entidades da Administração Pública com seguro contra incidentes de segurança das TIC, tendo passado de 5% em 2020 para 3% em 2021 (DGEEC).

EDUCAÇÃO E SENSIBILIZAÇÃO EM PORTUGAL

A maioria das ações de sensibilização em cibersegurança realizadas por entidades com responsabilidades na matéria, em 2021, ocorreram através de sessões presenciais ou *online* (80%). Seguem-se as redes sociais (7,4%), os cursos *online* (6,4%) e outros meios como *websites* (6,2%). Há muito poucas ações nos meios de comunicação social (0,1%) (CNCS).

Em 2021, comparando as sessões presenciais ou *online* com os cursos *online* de sensibilização em cibersegurança, estes revelam alguma eficácia em termos do número de pessoas alcançadas (CNCS).

Os jovens adultos (19-29 anos) e os adultos (30-64) foram as faixas etárias que predominaram como públicos-alvo das ações de sensibilização em cibersegurança, em 2021 e 2022 (até ao 1o semestre). Não se verifica o predomínio de um sexo. (CNCS).

Os temas que predominaram como conteúdos das ações de sensibilização em cibersegurança, em 2021 e 2022 (até ao 1o semestre), foram as "Boas práticas genéricas de ciber-higiene", os "Riscos *online* e cibercrime" e a "Proteção de dados, privacidade e direitos" (CNCS).

Somente 33% das organizações estudadas que realizaram ações de sensibilização em cibersegurança, em 2021 e 2022 (até ao 1o semestre), analisaram os impactos das mesmas no comportamento dos seus públicos-alvo (CNCS).

Somente 22% das PME em Portugal realizou ações de formação ou de consciencialização para os seus funcionários sobre os riscos do cibercrime, nos últimos 12 meses, em 2021. Este valor, ainda assim, é superior à média da UE, que se fixa em 19% (Eurobarómetro).

Na Administração Pública, em 2021, as ações de formação dos funcionários para a consciencialização das suas obrigações em matéria de segurança das TIC foram, na sua maioria, voluntárias, estando estas presentes em 67% dos organismos (mais 2 pp do que no ano anterior). As ações obrigatórias aumentaram a sua percentagem de 22% em 2020 para 26% em 2021 (DGEEC).

Registaram-se mais 3 cursos superiores especializados em cibersegurança e segurança de informação em Portugal, em 2022, todos eles TESP, perfazendo um total de 25: 13 TESP, uma licenciatura, 10 mestrados e um doutoramento (DGES: recolha CNCS).

Em termos de distribuição regional, em 2022, 44% dos cursos especializados em cibersegurança e segurança de informação concentram-se no Norte do país, 28% na Área Metropolitana de Lisboa, 20% no Centro e 8% no Alentejo (DGES: recolha CNCS).

Verificou-se um crescimento de 28% no número de alunos inscritos em cursos especializados em cibersegurança e segurança de informação no ano letivo de 2021/2022, de 718 para 916. Entre os alunos inscritos, 10% são mulheres (mais 2 pp do que no ano anterior) (DGEEC: recolha CNCS).

No ano letivo de 2020/2021, o número de alunos diplomados em cursos especializados em cibersegurança e segurança de informação decresceu 14%, de 152 para 130. Entre os alunos diplomados, 6% são mulheres (menos 3 pp do que no ano anterior) (DGEEC: recolha CNCS).

> A IMPORTÂNCIA DO FATOR HUMANO NA CIBERSEGURANÇA EXIGE UM ACOMPANHAMENTO CONTÍNUO DA SUA EVOLUÇÃO DE MODO A IDENTIFICAR INSUFICIÊNCIAS E TENDÊNCIAS

B. INTRODUÇÃO

A importância do fator humano na cibersegurança exige um acompanhamento contínuo da sua evolução de modo a identificar insuficiências e tendências. Esta componente é relevante quer do ponto de vista das competências transversais, importantes em qualquer utilizador e na sua ciber-higiene, quer no que diz respeito a competências em profundidade, necessárias em especialistas em cibersegurança. O *Relatório Cibersegurança em Portugal, tema Sociedade 2022*, a quarta edição deste documento, procura tratar estas duas dimensões de competências, tendo em consideração os indivíduos e as organizações, o setor privado e a Administração Pública.

Este relatório divide-se em quatro capítulos principais: ambiente sociotécnico, no qual se analisam os usos da Internet e de serviços considerados críticos para a cibersegurança, de modo a compreender o nível de exposição ao risco por parte dos utilizadores em Portugal; interesse pela "cibersegurança" nas pesquisas *online*, em que se examinam as pesquisas sobre este termo em Portugal, bem como a sua distribuição regional e palavras paralelas, com o objetivo de compreender a notoriedade do tema neste contexto; atitudes e comportamentos, capítulo no qual se consideram os dados disponíveis sobre os indivíduos e as organizações, nomeadamente a gestão dos dados pessoais e compras *online*, as PME na sua relação com o cibercrime e a cibersegurança na Administração Pública; e, por fim, sensibilização e educação, em que se caracterizam as ações de sensibilização realizadas em Portugal, bem como os cursos e os alunos inscritos e diplomados no ensino superior de cibersegurança e segurança de informação.

Além destes capítulos de análise nuclear, o relatório apresenta uma secção complementar sobre a ENSC e a sua articulação com os indicadores considerados no documento, procurando conjeturar sobre possíveis impactos e necessidades estratégicas. Seguem-se um conjunto de recomendações práticas tendo em conta os principais problemas identificados, as notas conclusivas e as notas metodológicas, além de outros aspetos ligados à construção e leitura do documento. Como anexo é possível encontrar uma lista das linhas de ação da ENSC com as quais este relatório se articula.

Em termos metodológicos, tal como nas edições anteriores, recorre-se a estatísticas disponíveis, a informações públicas por sistematizar e a dados próprios produzidos através de inquérito. O objetivo é conseguir uma visão integrada relativamente ao ano principal em apreço, o de 2021.

“NO QUE DIZ RESPEITO AO USO DA INTERNET, VERIFICA-SE UM EVIDENTE AUMENTO DA INTENSIDADE DE USO E DO NÚMERO DE UTILIZADORES”

C. AMBIENTE SOCIOTÉCNICO

Os usos das tecnologias digitais e da Internet em particular devem ser considerados quando se analisam os comportamentos ligados à ciber-higiene. Um maior uso destes dispositivos e sistemas representa uma maior exposição aos seus eventuais riscos, logo, uma maior necessidade de aplicar boas práticas de segurança. A estes usos chama-se neste documento "ambiente sociotécnico"[1].

O USO DA INTERNET

No que diz respeito ao uso da Internet, verifica-se um evidente aumento da intensidade de uso e do número de utilizadores. O tráfego médio dos dados fixos por acesso, segundo a Autoridade Nacional de Comunicações (ANACOM), mostra um claro incremento. Se em 2020 este tráfego aumentou 55%, em 2021 atingiram-se mais 21%, comparando com o ano anterior. Segundo a mesma fonte, estes valores resultam de um efeito global da pandemia na ordem dos 33%, em que os períodos de maior confinamento social registaram um impacto de 43%. Há uma correlação entre o maior confinamento social, fruto da pandemia da Covid-19, e a intensificação do uso destes dados. No que diz respeito aos dados móveis, o consumo médio de Internet móvel por utilizador cresceu 25% em 2021, quando em 2020 já havia aumentado 24%, face ao ano anterior (ANACOM, 2022).

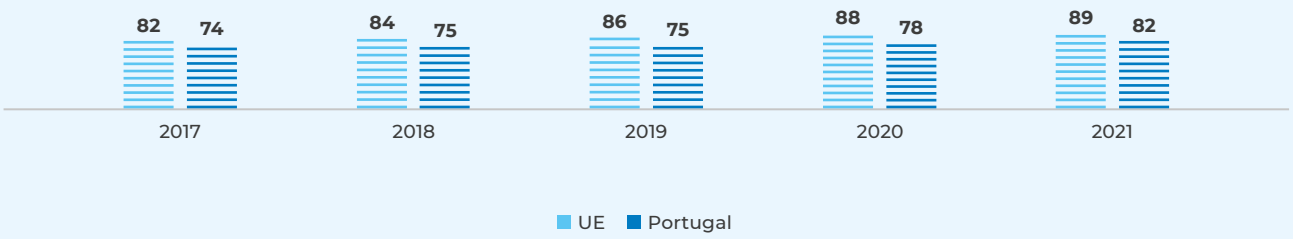
Segundo dados do Eurostat (2021a), o uso da Internet, nos últimos 3 meses, por parte de indivíduos[2] em Portugal, aumentou 4 pontos percentuais (pp) em 2021, comparando com 2020, passando de 78% para 82% dos indivíduos. No período pré-pandemia, em 2018 e 2019, o valor a este respeito apresentava-se estabilizado nos 75%. Portugal mantém-se, contudo, 7 pp abaixo da média da UE em 2021.

Esta tendência de crescimento terá relação com a pandemia da Covid-19 e com a crescente necessidade de serviços digitais provocada pelo trabalho remoto e pelos confinamentos sociais.

1. "Ambiente sociotécnico" é entendido neste âmbito como referência aos indicadores de usos de tecnologias com destaque para as suas implicações sociais num dado contexto.
2. Os dados do Eurostat respeitantes a indivíduos apresentados daqui em diante referem-se a indivíduos com idades compreendidas entre os 16 e os 74 anos.

Figura 1

INDIVÍDUOS QUE USARAM A INTERNET NOS ÚLTIMOS TRÊS MESES (%)*



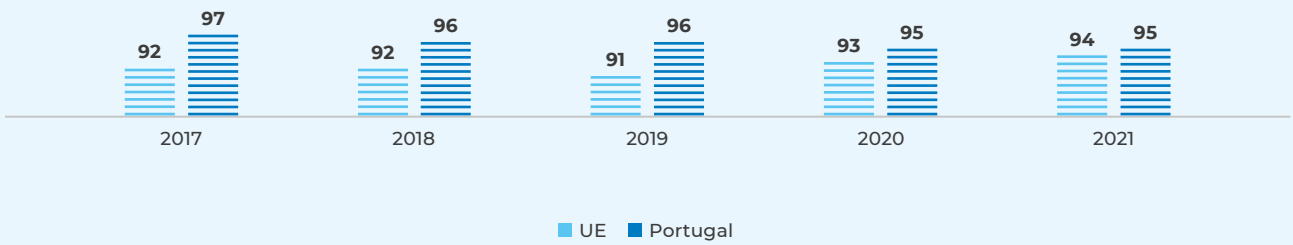
*Até 2019 os dados são referentes à UE a 28, a partir de 2020 passou a considerar-se os dados referentes à UE a 27.

Fonte: Eurostat, 2021a

Nas empresas assiste-se a uma maior estabilidade nos valores. Em 2021, 95% das empresas usavam DSL (Digital Subscriber Line) ou outra conexão de banda larga, mais 1 pp do que na média da UE e um valor igual a 2020 (Eurostat, 2021b). Portanto, as grandes mudanças no uso da Internet em termos de número de utilizadores verificaram-se mais nos indivíduos do que nas organizações.

Figura 2

EMPRESAS QUE USARAM DSL OU OUTRA CONECÇÃO DE BANDA LARGA (%)*



*Até 2019 os dados são referentes à UE a 28, a partir de 2020 passou a considerar-se os dados referentes à UE a 27.

Fonte: Eurostat, 2021b

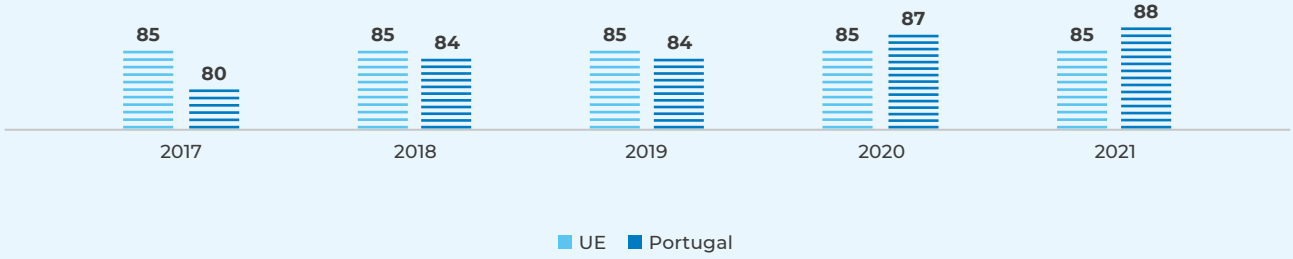
OS USOS DE SERVIÇOS CRÍTICOS PARA A CIBERSEGURANÇA

Existem alguns serviços *online* que representam vetores de vulnerabilidade de cibersegurança por via do comportamento humano. Por essa razão, é importante analisar a evolução do uso destes serviços de modo a considerar a exposição dos utilizadores aos riscos que uma má utilização pode implicar. Consideram-se de seguida o *email*, os telefonemas e videochamadas via Internet, as redes sociais, o banco *online*, as mensagens instantâneas e as compras *online* (no que diz respeito aos últimos três meses) (Eurostat, 2021c).

Em Portugal, no ano de 2021, o uso de *email* aumentou 1 pp em relação ao ano anterior. Desde 2020 que existem mais indivíduos a usar *email* no país do que a média da UE.

Figura 3

INDIVÍDUOS QUE USARAM EMAIL NOS ÚLTIMOS TRÊS MESES (%)*



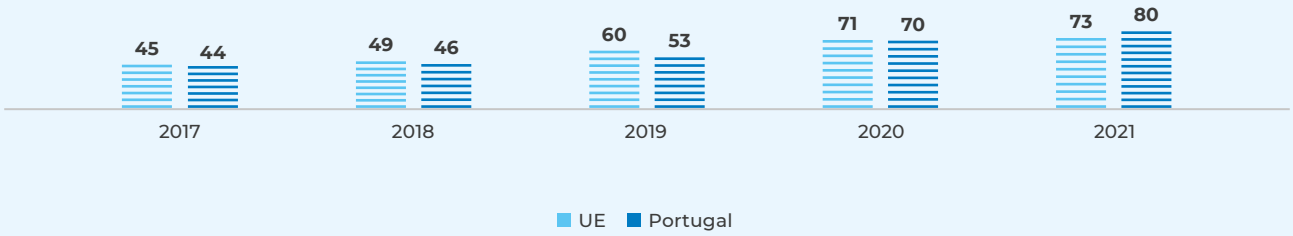
*Até 2019 os dados são referentes à UE a 28, a partir de 2020 passou a considerar-se os dados referentes à UE a 27.

Fonte: Eurostat, 2021c

Considerando o uso de telefone e videochamadas via Internet, verifica-se um aumento muito acentuado, de 10 pp, passando-se de 70% dos indivíduos em 2020 para 80% em 2021, sendo que em 2020 já se havia assistido a um incremento de 17 pp. Pela primeira vez nos últimos 5 anos, Portugal está acima da média da UE, com mais 7 pp, a este respeito.

Figura 4

INDIVÍDUOS QUE USARAM TELEFONE E VÍDEOCHAMADAS VIA INTERNET NOS ÚLTIMOS TRÊS MESES (%)*



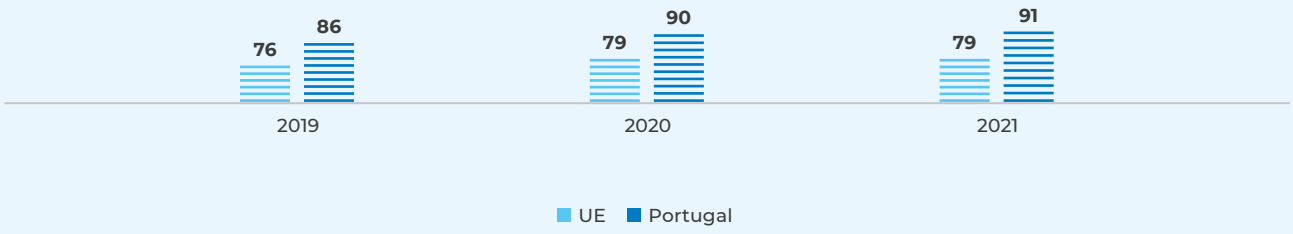
*Até 2019 os dados são referentes à UE a 28, a partir de 2020 passou a considerar-se os dados referentes à UE a 27.

Fonte: Eurostat, 2021c

O uso de mensagens instantâneas em Portugal também é bastante frequente comparando com a média da UE. Em 2021, verificou-se um ligeiro aumento de 1 pp em relação a 2020, para 91% dos indivíduos, mais 12 pp do que a média da UE.

Figura 5

INDIVÍDUOS QUE USARAM MENSAGENS INSTANTÂNEAS NOS ÚLTIMOS TRÊS MESES (%)*



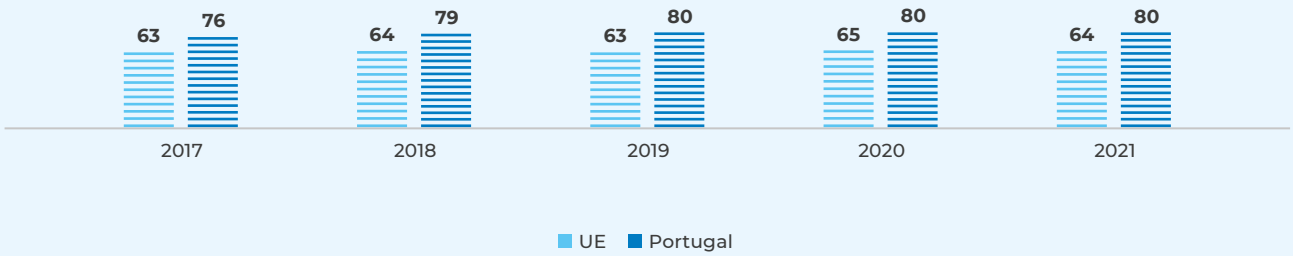
*Até 2019 os dados são referentes à UE a 28, a partir de 2020 passou a considerar-se os dados referentes à UE a 27.

Fonte: Eurostat, 2021c

Outro ponto crítico são as redes sociais. Neste aspeto, Portugal apresenta os mesmos valores desde 2019, isto é, 80% dos indivíduos a usarem estas plataformas. Em 2021, a distância relativamente à média da UE continua a ser significativa, com 16 pp acima do registo da UE.

Figura 6

INDIVÍDUOS QUE USARAM REDES SOCIAIS NOS ÚLTIMOS TRÊS MESES (%)*



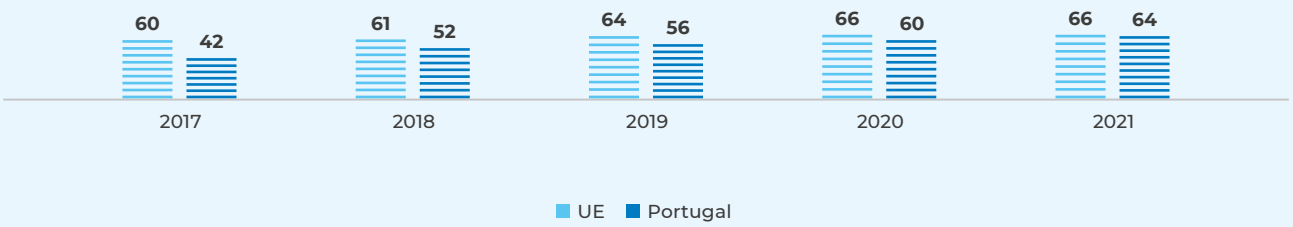
*Até 2019 os dados são referentes à UE a 28, a partir de 2020 passou a considerar-se os dados referentes à UE a 27.

Fonte: Eurostat, 2021c

No que diz respeito ao serviço de banco *online* em 2021, verifica-se, em Portugal, a existência de 64% de indivíduos a utilizarem este tipo de plataforma, um aumento de 4 pp em relação ao ano anterior. Esta variação aproximou o país dos valores da média da UE, de 66%. De referir que se verifica em Portugal um aumento consistente desta percentagem desde pelo menos 2017 (crescimento contínuo que se inicia em 2014).

Figura 7

INDIVÍDUOS QUE USARAM BANCO *ONLINE* NOS ÚLTIMOS TRÊS MESES (%)*



*Até 2019 os dados são referentes à UE a 28, a partir de 2020 passou a considerar-se os dados referentes à UE a 27.

Fonte: Eurostat, 2021c

Por fim, em Portugal, no ano de 2021, realizaram-se muito menos compras *online* do que a média da UE: 40% dos indivíduos em Portugal e 57% na média da UE. Todavia, no mesmo ano, registou-se um aumento de 5 pp em relação ao ano anterior, em que o valor era de 35%.

Figura 8

INDIVÍDUOS QUE REALIZARAM COMPRAS *ONLINE* NOS ÚLTIMOS TRÊS MESES (%)

Fonte: Eurostat, 2021c

DESTAQUES

- Verifica-se um aumento no uso da Internet em 2021, quer em termos de tráfego de dados (mais 21% de dados fixos e mais 25% de dados móveis do que em 2020), quer de número de indivíduos que a utilizam (82% - mais 4 pp do que em 2020).
- Regista-se um aumento, em Portugal, no ano de 2021, de indivíduos a usar o *email* (mais 1 pp), o telefone e videochamadas através da Internet (mais 10 pp), as mensagens instantâneas (mais 1 pp) e o banco *online* (mais 4 pp).
- Com valores acima da média da UE, em Portugal, em 2021, encontram-se os usos das redes sociais (mais 16 pp), do *email* (mais 3 pp), dos telefonemas e videochamadas pela Internet (mais 7 pp) e das mensagens instantâneas (mais 12 pp).

ÍNDICE DE AMBIENTE SOCIOTÉCNICO

Internet em 2021 – aumento do uso.

Aspetos críticos em 2021 – aumento significativo do uso do telefone e videochamadas através da Internet e do banco *online*; manutenção de um uso muito elevado de redes sociais e de mensagens instantâneas.

“EM PORTUGAL, O INTERESSE PELA CIBERSEGURANÇA NAS PESQUISAS *ONLINE* AUMENTOU ENTRE 2019 E 2020, DECRESCENDO LIGEIRAMENTE EM 2021, SEM VOLTAR AOS VALORES PRÉ-PANDEMIA. NO PRIMEIRO SEMESTRE DE 2022, ESTE INTERESSE CRESCEU DE FORMA EXPONENCIAL”

D. INTERESSE PELA "CIBERSEGURANÇA" NAS PESQUISAS *ONLINE*

Um dos métodos disponíveis para determinar o interesse social na cibersegurança em Portugal é mediante a análise das pesquisas *online* relativas à palavra-chave "cibersegurança". Com este propósito analisou-se a frequência das pesquisas *online* com este termo no motor de busca Google, mediante o instrumento Google Trends.

PESQUISAS PELA PALAVRA "CIBERSEGURANÇA"

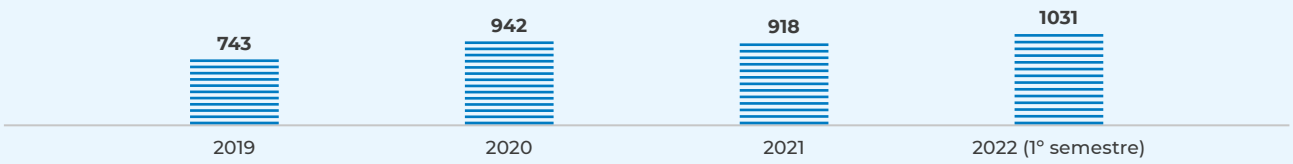
Com base nos valores respeitantes à intensidade de pesquisas (o número de pesquisas convertidos em níveis, em que 0 é baixo e 100 é alto)[3] apresentados por esta plataforma relativamente a cada semana desde 2019, e somando esses valores, observa-se que em 2020 assistiu-se a um aumento no nível de interesse por este tema no que a pesquisas no Google diz respeito. Em 2021, esse nível diminuiu ligeiramente, mas sem voltar aos valores de 2019. Todavia, verifica-se que no primeiro semestre de 2022 este interesse aumentou de modo muito significativo, visto terem sido atingidos valores superiores aos do ano todo anterior.

O aumento do interesse por esta matéria em 2020 poderá ser explicado pelo emergir da pandemia da Covid-19 e das necessidades de cibersegurança provocadas pela massificação do trabalho remoto e do uso de certos serviços digitais. O aumento registado no primeiro semestre de 2022 estará, eventualmente, relacionado com alguns casos mediáticos e com impacto, como os ataques às organizações Impresa em janeiro e Vodafone em fevereiro.

3. "Os números representam o interesse de pesquisa relativo ao ponto mais alto do gráfico para a região e o intervalo de tempo especificados. Um valor de 100 é o pico de popularidade do termo. Um valor de 50 significa que o termo teve metade da popularidade. Uma pontuação de 0 significa que não houve dados suficientes para este termo" (Google Trends). Os valores apresentados nos gráficos resultam da soma dos valores semanais apresentados pelo Google Trends segundo a lógica descrita.

Figura 9

NÍVEL DE INTERESSE* NA PESQUISA PELA PALAVRA "CIBERSEGURANÇA" NO MOTOR DE BUSCA GOOGLE, EM PORTUGAL, POR ANO



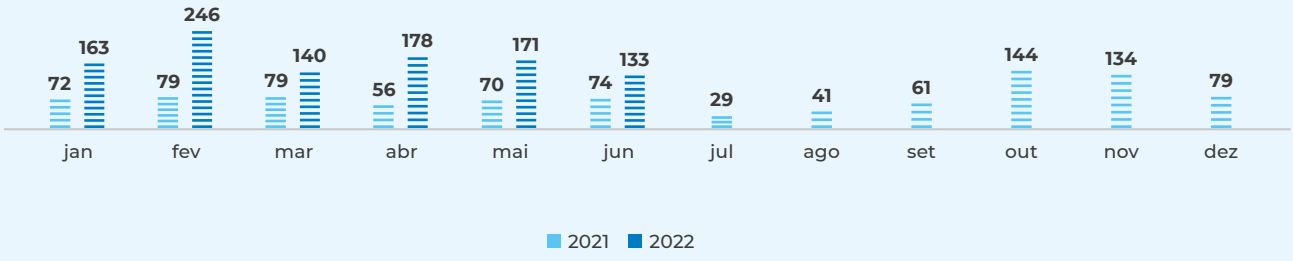
* Nível de interesse: soma dos valores semanais, entre 0 e 100, em que 0 significa sem interesse e 100 muito interesse.

Fonte: Google Trends

Observando as variações mensais de 2021 e do primeiro semestre de 2022, verifica-se a importância do mês de fevereiro de 2022, com um nível de interesse muito superior aos restantes meses. Qualquer mês do primeiro semestre de 2022 apresenta resultados superiores ao período homólogo. Durante o ano de 2021, os meses de outubro e novembro foram os que apresentaram valores de interesse mais elevados, os únicos com níveis semelhantes a alguns dos meses do primeiro semestre de 2022.

Figura 10

NÍVEL DE INTERESSE* NA PESQUISA PELA PALAVRA "CIBERSEGURANÇA" NO MOTOR DE BUSCA GOOGLE, EM PORTUGAL, POR MÊS



* Nível de interesse: soma dos valores semanais, entre 0 e 100, em que 0 significa sem interesse e 100 muito interesse.

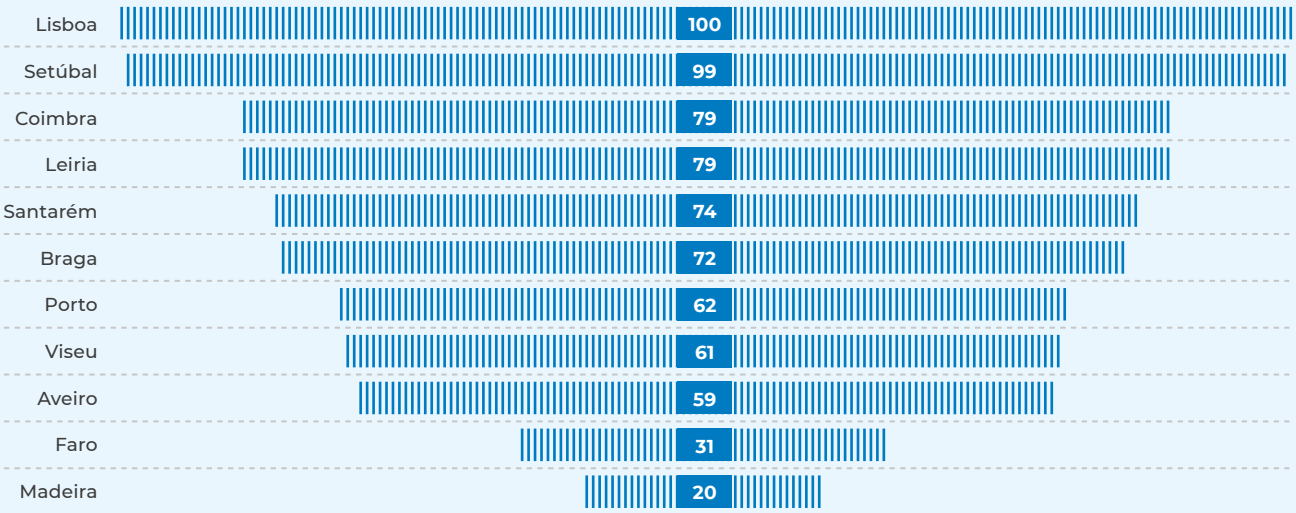
Fonte: Google Trends

DISTRIBUIÇÃO REGIONAL DAS PESQUISAS *ONLINE* E TERMOS PARALELOS

O interesse pela pesquisa da palavra "cibersegurança" não se distribui geograficamente pelo país com pesos iguais, tendo em conta o período entre 2019 e o primeiro semestre de 2022. O distrito de Lisboa é onde se verifica mais interesse em termos relativos, seguido de Setúbal e Coimbra. O Porto, embora a segunda cidade mais populosa do país, surge na sétima posição nesta matéria. Este cálculo é proporcional à dimensão populacional da região e não representa os números absolutos sobre as consultas efetuadas.

Figura 11

NÍVEL DE INTERESSE NA PESQUISA PELA PALAVRA "CIBERSEGURANÇA" NO MOTOR DE BUSCA GOOGLE, EM PORTUGAL, POR DISTRITO E REGIÃO AUTÓNOMA*, 2019-2022 (1ºSEM.)



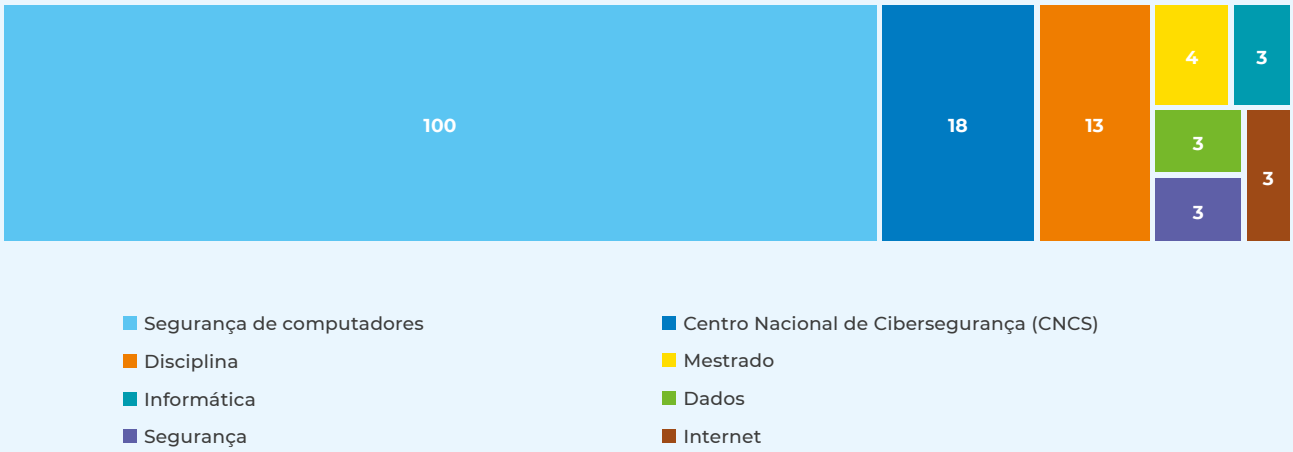
* Apenas regiões com mais de zero. "Observação: um valor maior significa uma proporção maior de consultas, não uma contagem absoluta maior" (Google Trends).

Fonte: Google Trends

Quem pesquisou pela palavra "cibersegurança" também pesquisou por outros tópicos associados. Considerando os mais frequentes, verifica-se a predominância dos tópicos "segurança de computadores", conceito que se pode considerar sinónimo de "cibersegurança", seguido de "Centro Nacional de Cibersegurança", o que revela um interesse pela instituição, e do tópico "disciplina", o qual, juntamente com o tópico "mestrado", revela um interesse pela educação nesta área.

Figura 12

NÍVEL DE INTERESSE POR TÓPICOS RELACIONADOS DE QUEM PESQUISOU PELA PALAVRA "CIBERSEGURANÇA" NO MOTOR DE BUSCA GOOGLE, EM PORTUGAL, 2019-2022 (1º SEM.)



Fonte: Google Trends

DESTAQUES

- Em Portugal, o interesse pela "cibersegurança" nas pesquisas *on-line* aumentou entre 2019 e 2020, decrescendo ligeiramente em 2021, sem voltar aos valores pré-pandemia. No primeiro semestre de 2022, este interesse cresceu de forma exponencial.
- Os distritos de Lisboa, Setúbal e Coimbra são as regiões com mais interesse pelas pesquisas *online* da palavra "cibersegurança", proporcionalmente ao seu tamanho.
- O CNCS e a área da educação surgem como os tipos de tópicos relacionados mais relevantes.

“OS INDIVÍDUOS MAIS VELHOS E OS QUE TÊM FORMAÇÃO BÁSICA TENDEM A AFIRMAR TER MENOS CUIDADOS EM TERMOS DE PRIVACIDADE E PROTEÇÃO DE DADOS *ONLINE* DO QUE OS JOVENS E DO QUE OS QUE TÊM FORMAÇÃO SUPERIOR”

E. ATITUDES E COMPORTAMENTOS

Os indivíduos e as organizações são possíveis vítimas de ameaças no ciberespaço de natureza diferente. Se os indivíduos são vítimas predominantemente de ataques como o *phishing* ou a burla *online*, as organizações são mais atacadas por incidentes como o *ransomware* ou a exfiltração de dados. Todavia, as organizações são constituídas por indivíduos e alguns incidentes de *ransomware*, por exemplo, podem começar com o envio de um *email* e o clique num anexo malicioso por parte de um indivíduo. Por isso, existe uma contaminação entre a vida profissional e a vida privada no ciberespaço. Neste capítulo, consideram-se as atitudes e os comportamentos dos indivíduos e das organizações (em particular PME e Administração Pública).

Tendo em conta os dados estatísticos disponíveis relativos a Portugal em 2021, considera-se de seguida a gestão dos dados pessoais *online* por parte dos indivíduos, bem como as barreiras e problemas de segurança que estes encontraram nas compras *online*, analisando estatísticas do Eurostat (2021d e 2021e); seguindo-se uma análise às PME e cibercrime, recorrendo a um inquérito do Eurobarómetro (2022); e, por fim, uma abordagem à Administração Pública Central, Regional e Câmaras Municipais (conjunto que se designará de "Administração Pública"), com base em dois inquéritos anuais produzidos pela Direção-Geral de Estatísticas da Educação e Ciência (DGEEC) (2022a e 2022b).

PRIVACIDADE E PROTEÇÃO DOS DADOS PESSOAIS *ONLINE*

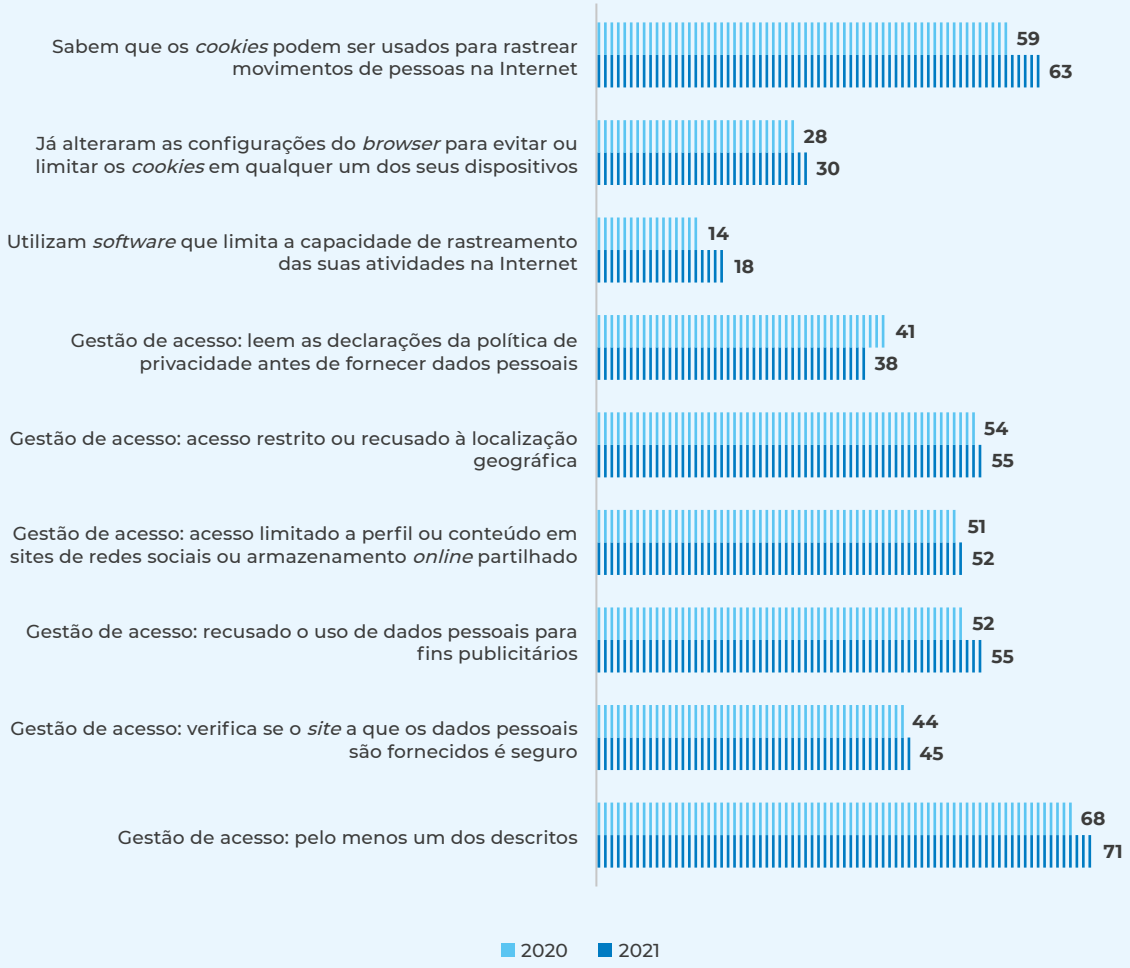
Os indicadores do Eurostat (2021e) *Privacidade e proteção de dados* pessoais, já analisados na edição do ano passado deste relatório (CNCS, 2021b), permitem acompanhar os cuidados que os indivíduos têm com os seus dados pessoais *online*, tendo em conta os últimos três meses. A reedição deste inquérito em 2021 possibilita fazer comparações com o ano anterior.

Em Portugal, no ano de 2021, 71% dos indivíduos utilizaram pelo menos um dos métodos de gestão do acesso aos dados pessoais na Internet descritos no inquérito, mais 3 pp do que no ano anterior. Também se verificou um aumento nas percentagens dos indivíduos que sabem que os *cookies* podem ser usados para rastrear movimentos de pessoas na Internet (63% - mais 4 pp do que no ano anterior); dos indivíduos que alteraram as configurações do *browser* para evitar ou limitar os *cookies* (30% - mais 2 pp do que no ano anterior); e dos indivíduos que utilizaram *software* que limita a capacidade de rastreamento das suas atividades na Internet (18% - mais 4 pp do que no ano anterior).

Na gestão do acesso aos dados pessoais na Internet, os cuidados mais comuns foram a restrição ou recusa do acesso à localização (55% - mais 1 pp do que no ano anterior) e a recusa do uso dos dados pessoais para fins publicitários (55% - mais 3 pp do que no ano anterior). Verificou-se um decréscimo apenas na percentagem de indivíduos que leem as declarações da política de privacidade antes de fornecerem os seus dados pessoais (38% - menos 3 pp do que no ano anterior).

Figura 13

PRIVACIDADE E PROTEÇÃO DOS DADOS PESSOAIS *ONLINE*, PORTUGAL, PELOS INDIVÍDUOS, NOS ÚLTIMOS TRÊS MESES (%)



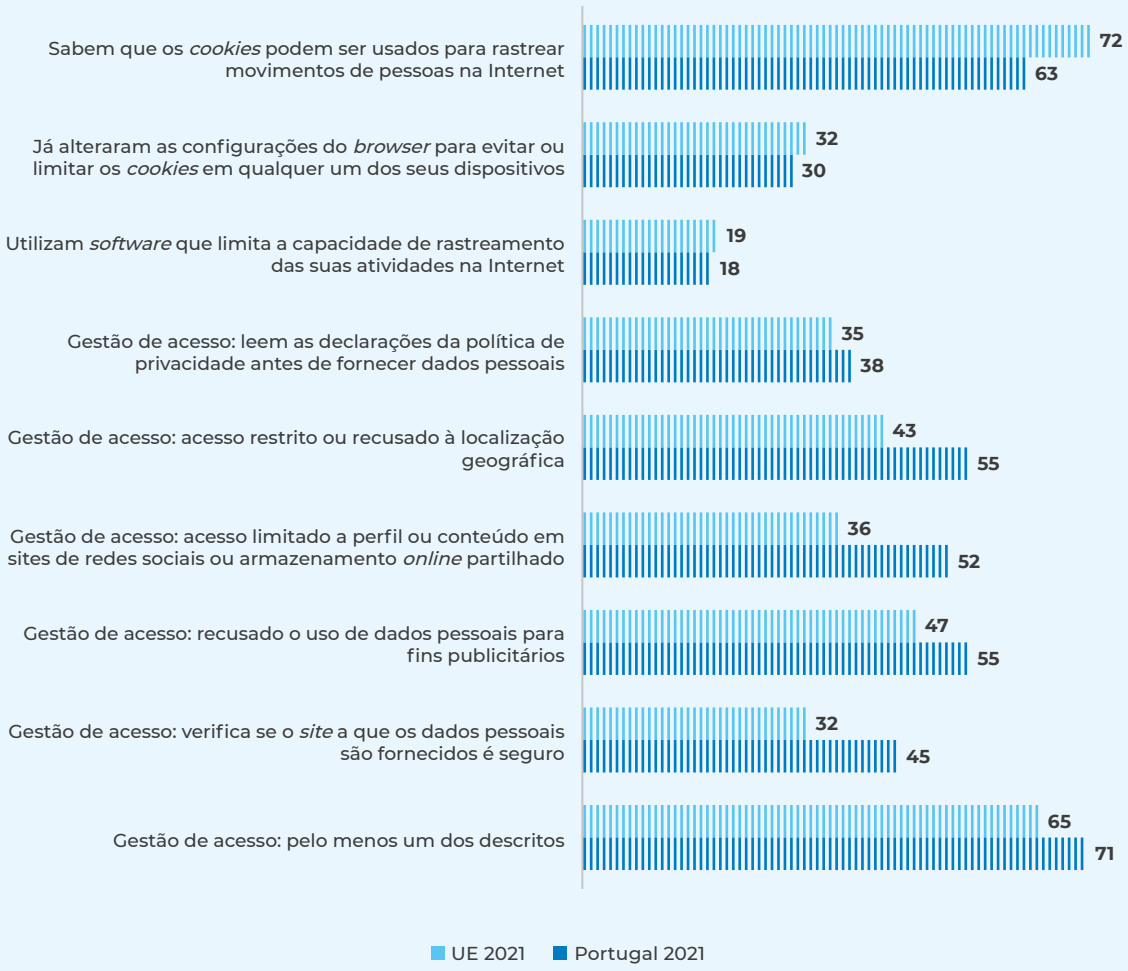
Fonte: Eurostat, 2021e

Comparando estes resultados de Portugal com a média da UE, verifica-se que em 2021, em Portugal, há mais indivíduos que gerem os dados pessoais na Internet do que a média da UE (71% em Portugal e 65% na média da UE aplicaram pelo menos um dos cuidados), o que se reflete em todos os cuidados descritos, nos quais os indivíduos em Portugal surgem sempre acima da média da UE.

Os indivíduos em Portugal apresentam resultados abaixo da média da UE no que diz respeito ao conhecimento sobre os *cookies* (menos 9 pp) e ações que limitam estes mesmos *cookies* através do *browser* (menos 2 pp), embora o país apresente uma tendência positiva em ambos os casos, como se referiu.

Figura 14

PRIVACIDADE E PROTEÇÃO DOS DADOS PESSOAIS *ONLINE*, UE E PORTUGAL, PELOS INDIVÍDUOS, NOS ÚLTIMOS TRÊS MESES (%)

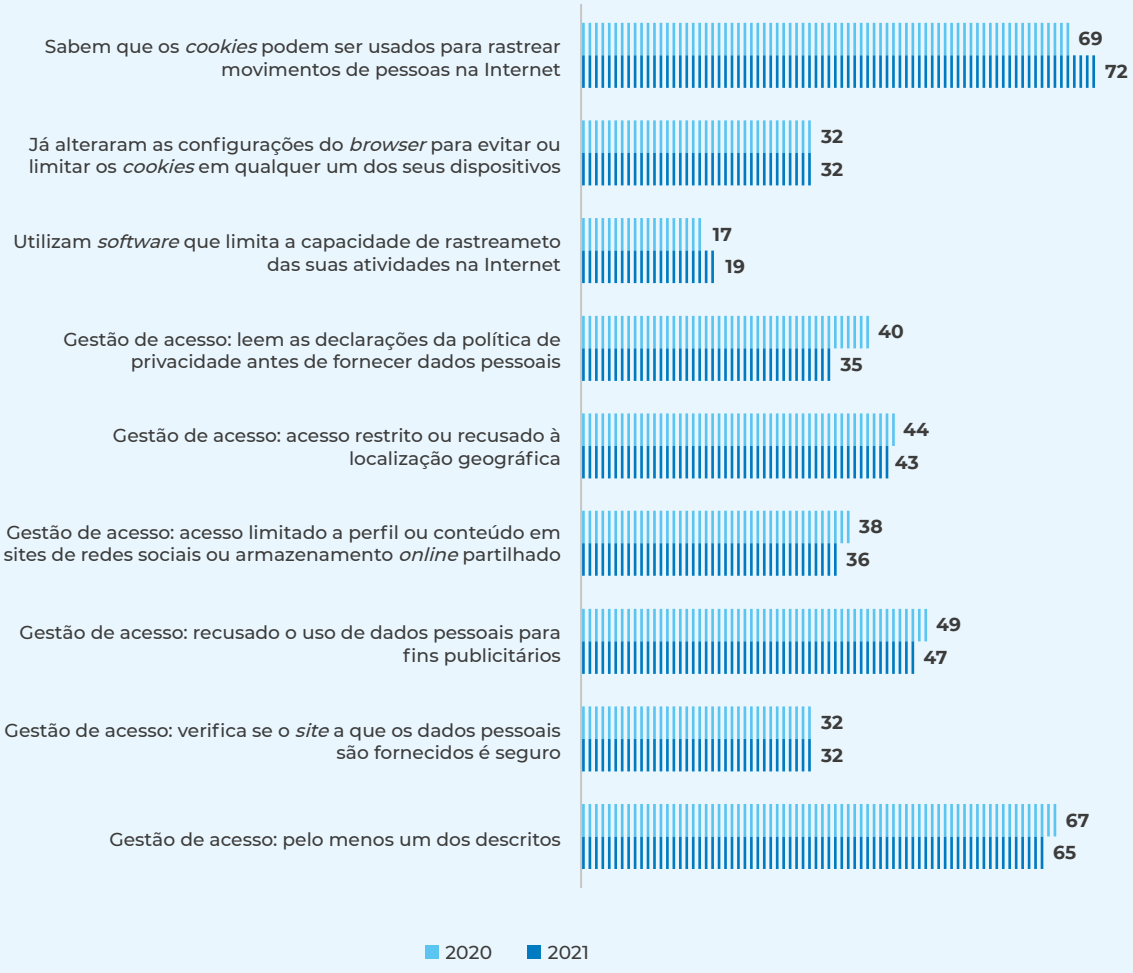


Fonte: Eurostat, 2021e

Quanto à evolução da média da UE a este respeito, verifica-se uma tendência de aumento relativamente ao conhecimento sobre o que fazem os *cookies* (mais 3 pp do que no ano anterior) e à utilização de *software* que limita o rastreamento *online* (mais 2 pp). Não obstante, a tendência é de decrescimento no que se refere à gestão dos dados pessoais na Internet em geral (menos 2 pp entre os que aplicaram pelo menos uma das ações descritas).

Figura 15

PRIVACIDADE E PROTEÇÃO DOS DADOS PESSOAIS *ONLINE*, UE, PELOS INDIVÍDUOS, NOS ÚLTIMOS TRÊS MESES (%)



Fonte: Eurostat, 2021e

ASPETOS SOCIODEMOGRÁFICOS RELEVANTES EM PORTUGAL, 2021

Sexo	**Valores semelhantes entre os sexos feminino e masculino quanto aos cuidados relativamente à privacidade e proteção de dados *online***, exceto no que diz respeito a configurações do *browser* para evitar ou limitar os *cookies*, que os indivíduos do sexo masculino tendem a aplicar mais (35% entre os homens e 26% entre as mulheres)
Idade	**Os indivíduos mais velhos tendem a ter menos cuidados relativamente à privacidade e proteção dos seus dados *online* do que os mais jovens.** Por exemplo, 94% dos indivíduos com idades entre os 16 e os 24 anos já aplicaram pelo menos uma das medidas de gestão do acesso aos dados pessoais na Internet, mas apenas 32% dos indivíduos com idades entre os 65 e 74 anos o fizeram.
Educação	**Os indivíduos com formação básica tendem a ter menos cuidados relativamente à privacidade e proteção de dados *online* do que os que têm uma formação superior.** Por exemplo, 95% dos indivíduos com formação superior já aplicaram pelo menos uma das medidas de gestão do acesso aos dados pessoais na Internet, mas somente 46% dos que têm formação básica o fizeram.
UE	**Valores genericamente alinhados com a UE, embora os indivíduos com formação média tenham mais cuidados em Portugal.** Por exemplo, em Portugal, 89% dos indivíduos com formação média já aplicaram pelo menos uma das medidas de gestão do acesso aos dados pessoais na Internet, enquanto a média da UE é de 63%.

DESTAQUES

- Em Portugal, no ano de 2021, há mais conhecimento sobre o que fazem os *cookies* do que no ano anterior (63% - mais 4 pp), embora mantendo-se este valor abaixo da média da UE (menos 9 pp).
- Também se verifica em 2021 a existência de mais cuidados com a gestão dos dados pessoais na Internet do que em 2020 (71% aplicaram pelo menos um dos cuidados - mais 3 pp), neste caso, colocando-se acima da média da UE (mais 6 pp).
- A média da UE aumentou no período em causa no que diz respeito ao conhecimento sobre o que fazem os *cookies* (mais 3 pp), mas encontra-se em sentido contrário relativamente à gestão dos dados pessoais na Internet (menos 2 pp).
- Os indivíduos mais velhos e os que têm formação básica tendem a afirmar ter menos cuidados em termos de privacidade e proteção de dados *online* do que os jovens e do que os que têm formação superior.

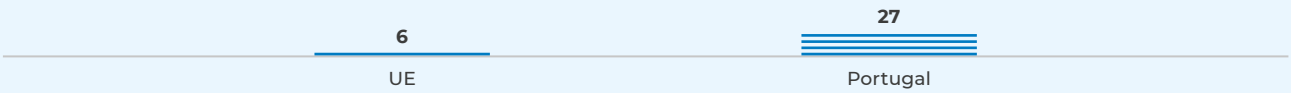
> Relação com as seguintes linhas de ação da ENSC: E2d, E2e, E2f e E2h (ver anexo).

COMPRAS *ONLINE* – BARREIRAS E PROBLEMAS DE SEGURANÇA

No âmbito das questões realizadas pelo Eurostat (2021d) acerca das *Compras online*, no seu inquérito sobre os usos das TIC no contexto familiar, verifica-se a existência de pelo menos duas perguntas relacionadas com a segurança que interessa ter em conta na análise ao comportamento dos indivíduos. Um dos dados mais relevantes é o que diz respeito às barreiras percebidas nas compras *online*, perceções que impedem que os indivíduos realizem esta prática. Em Portugal, 27% dos inquiridos manifestaram serem as preocupações com a segurança e a privacidade dos pagamentos uma barreira relevante, quando a média da UE é de 6%.

Figura 16

COMPRAS *ONLINE* PELOS INDIVÍDUOS - BARREIRAS PERCEBIDAS: PREOCUPAÇÕES COM A SEGURANÇA E A PRIVACIDADE DOS PAGAMENTOS, EM 2021, NOS ÚLTIMOS TRÊS MESES (%)



Fonte: Eurostat, 2021d

Com um valor mais residual surgem os dados sobre os problemas relacionados com fraudes encontrados por quem efetivamente realizou compras *online*. Apenas 1% das pessoas encontraram este tipo de problema, o mesmo valor que a média da UE. Esta discrepância no que se refere às pessoas que não compraram *online* por razões de segurança e privacidade dos pagamentos assinala um eventual desajuste entre um determinado receio (27% dos que não compraram *online* percecionam essa barreira) e o problema efetivo (apenas 1% dos que compraram *online* encontraram problemas de fraude).

Figura 17

COMPRAS *ONLINE* PELOS INDIVÍDUOS - PROBLEMAS ENCONTRADOS: FRAUDE, EM 2021, NOS ÚLTIMOS TRÊS MESES (%)

Fonte: Eurostat, 2021d

ASPETOS SOCIODEMOGRÁFICOS RELEVANTES EM PORTUGAL, 2021

Sexo	**Os indivíduos do sexo masculino tendem a identificar (ligeiramente mais) do que os do sexo feminino, como barreira às compras *online*, a preocupação com a segurança e a privacidade dos pagamentos.** Por exemplo, 28% dos indivíduos do sexo masculino têm esta preocupação, em comparação com apenas 25% dos indivíduos do sexo feminino.
Idade	**Não existem diferenças relevantes entre faixas etárias relativamente à preocupação com a segurança e a privacidade dos pagamentos nas compras *online*.** Por exemplo, 25% dos indivíduos com idades compreendidas entre os 16 e os 24 anos têm esta preocupação, valor que se fixa nos 26% nos que têm idades entre os 65 e 74 anos.
Educação	**Os indivíduos com formação básica tendem a identificar mais do que os que têm uma formação superior, como barreira às compras *online*, as preocupações com a segurança e a privacidade dos pagamentos.** Por exemplo, 35% dos indivíduos com formação básica têm essa preocupação, enquanto se registam apenas 18% entre os que têm formação superior.
UE	**Verificam-se algumas divergências entre os resultados de Portugal e da média da UE quanto às barreiras percecionadas às compras *online* por razões de segurança e privacidade dos pagamentos.** A média da UE apresenta um certo equilíbrio entre indivíduos do sexo masculino e do sexo feminino (5% e 6%, respetivamente) e maiores diferenças entre idades (entre os indivíduos com idades entre os 16 e os 24 anos regista-se 3% com esta preocupação, atingindo-se os 8% entre os que têm entre 65 e 74 anos).

DESTAQUES

- Durante 2021, em Portugal, 27% dos indivíduos percecionaram como barreira às compras *online* as preocupações com a segurança e a privacidade dos pagamentos, enquanto a média da UE é apenas de 6%.
- Por outro lado, apenas 1% dos indivíduos que realizaram compras *online* encontrou problemas relacionados com fraudes, o mesmo valor que a média da UE.
- Relacionando os dois resultados, assinale-se a discrepância entre o receio de 27% que não compraram *online* e o problema efetivamente encontrado por apenas 1% dos que compraram *online*. Uma diferença muito menor do que a da média da UE (de 6% para 1%, respetivamente).
- Relativamente às preocupações com a privacidade e a segurança dos pagamentos como barreiras às compras *online*, a tradicional diferença entre idades e níveis de formação não se verifica em Portugal: poucas diferenças entre idades, além de pessoas com menos formação a mostrarem-se mais preocupadas. Em Portugal, o nível de formação é decisivo a este respeito e não o nível etário. De referir que a não realização de compras *online* não é necessariamente uma boa prática de cibersegurança.

> Relação com as seguintes linhas de ação da ENSC: E2d, E2e, E2f e E2h (ver anexo).

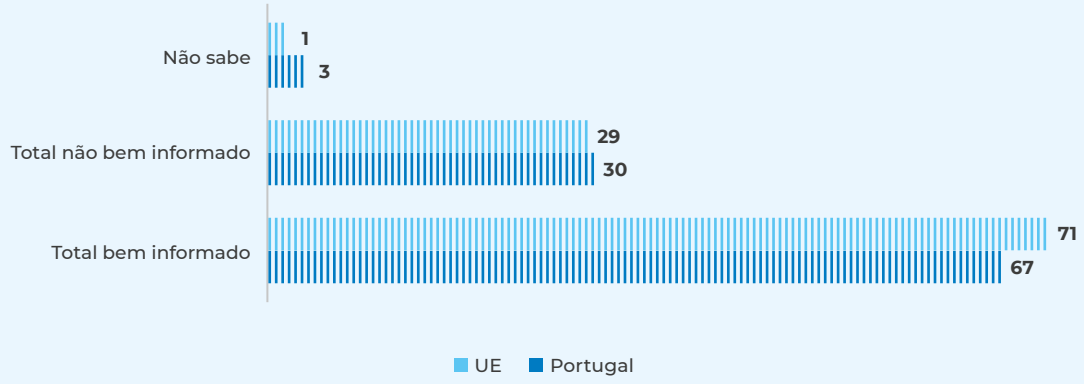
PME E CIBERCRIME

Com base nos resultados do Flash Eurobarómetro 496, sob o título *PME e Cibercrime*, é possível analisar algumas atitudes e comportamentos relativamente aos riscos de cibercrime por parte das PME europeias e portuguesas (Eurobarómetro, 2022). Um dos aspetos em consideração, tema que se repete noutros inquéritos do mesmo tipo, é a perceção de que os inquiridos (responsáveis de topo dentro da organização) têm sobre o seu próprio conhecimento e dos restantes colaboradores acerca do cibercrime.

Em Portugal, no ano de 2021, 67% dos inquiridos nas PME sentem-se bem informados sobre os riscos de cibercrime, menos 4 pp do que a média da UE, que atinge os 71%.

Figura 18

QUÃO BEM INFORMADO SE SENTE RELATIVAMENTE AOS RISCOS DE CIBERCRIME (2021)? *PME* (%)



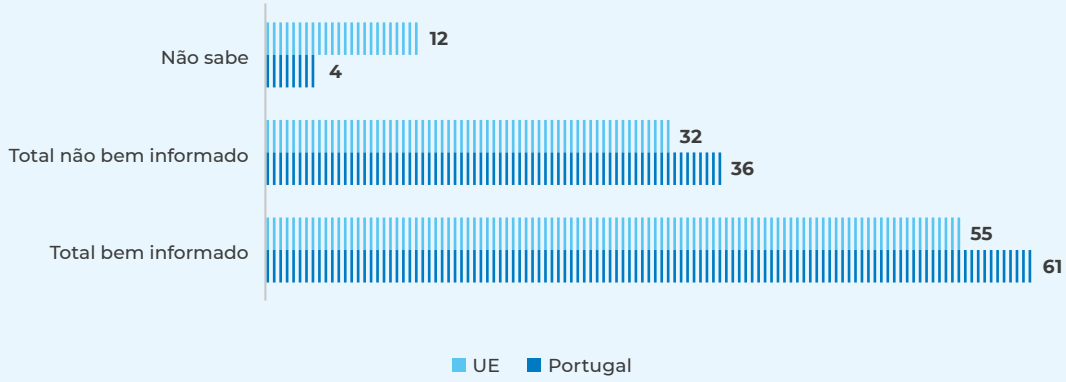
Fonte: Eurobarómetro, 2022

Em comparação com o modo como se veem a si próprios, são menos os inquiridos a considerarem que os restantes funcionários da empresa estão bem informados sobre esta matéria, num valor de 61% (recorde-se que em relação a si próprios atinge os 67%). Neste aspeto, os responsáveis de topo nas PME em Portugal têm uma perspetiva mais positiva relativamente aos restantes funcionários do que a média da UE, que se fica pelos 55%.

Quanto às preocupações com determinados riscos *online*, existem mais inquiridos de PME portuguesas do que a média da UE a manifestarem muita preocupação em relação a quase todos os tipos de riscos indicados no inquérito. A exceção é o *ransomware*, relativamente ao qual 21% dos inquiridos em Portugal manifestam muita preocupação, quando a média da UE é de 22%. O risco em relação ao qual existem mais inquiridos de PME portuguesas muito preocupados é o de *hacking* (ou tentativas) a contas bancárias *online*, para 55% das PME, contra 32% na média da UE (também o risco mais considerado).

Figura 19

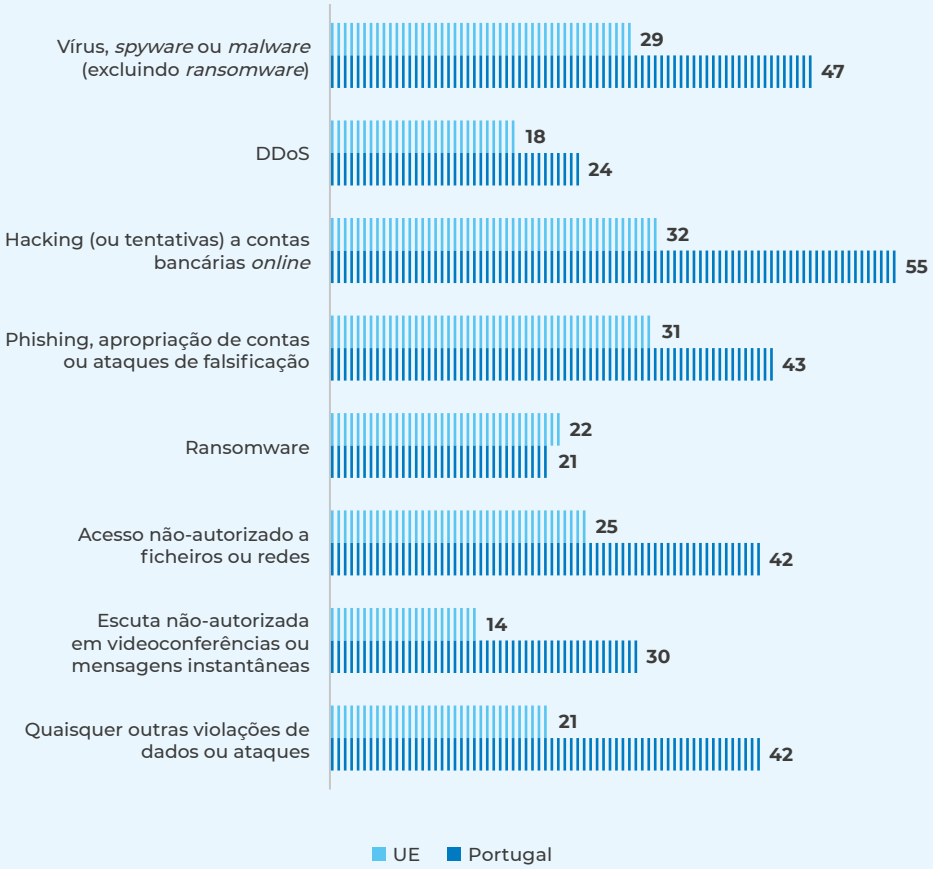
QUÃO BEM INFORMADOS SENTE QUE OS SEUS FUNCIONÁRIOS ESTÃO SOBRE OS RISCOS DO CIBERCRIME (2021)? *PME* (%)



Fonte: Eurobarómetro, 2022

Figura 20

AO UTILIZAR A INTERNET PARA ATIVIDADES RELACIONADAS COM A EMPRESA, COMO VENDA DE MERCADORIAS OU BANCA *ONLINE*, ESTÁ PREOCUPADO COM ALGUM DOS SEGUINTES RISCOS? (MUITO PREOCUPADO) *PME* (%)

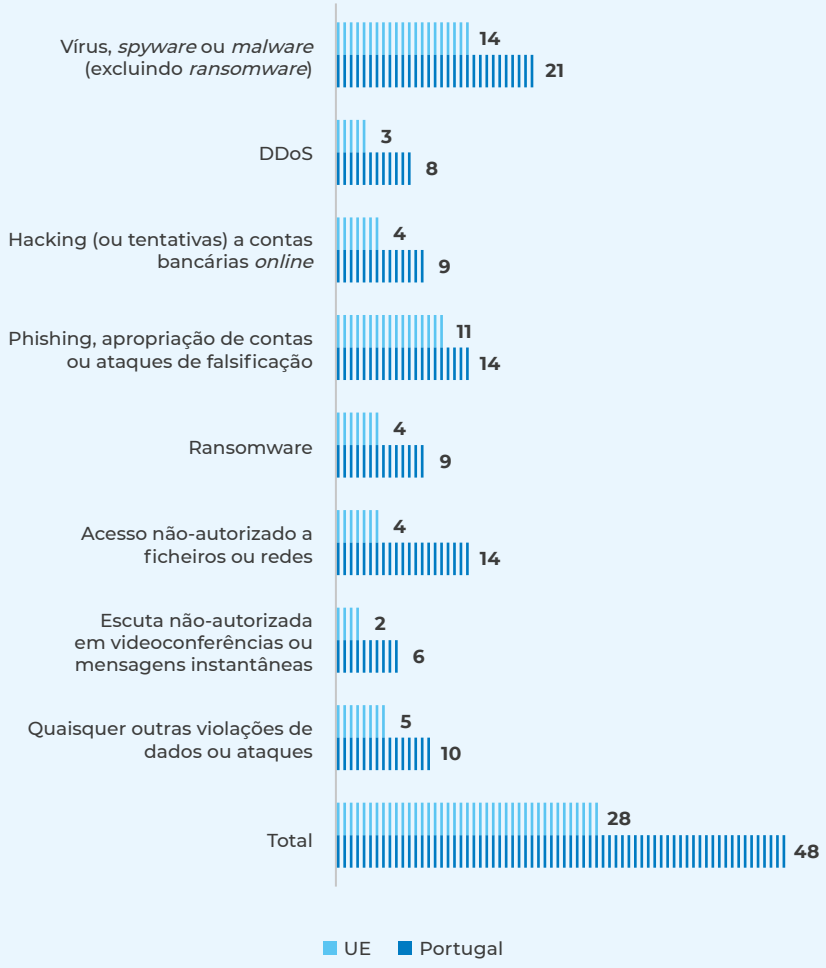


Fonte: Eurobarómetro, 2022

Sobre se alguma vez a PME do inquirido sofreu algum dos cibercrimes identificados, 48% em Portugal dizem já ter sofrido pelo menos um, enquanto a média da UE fica pelos 28%. O tipo de cibercrime mais sofrido nas PME portuguesas é o vírus, *spyware* ou *malware*, para 21% dos respondentes, mais 7 pp do que a média da UE.

Figura 21

A SUA EMPRESA SOFREU ALGUM DOS SEGUINTES TIPOS DE CIBERCRIME NOS ÚLTIMOS 12 MESES (2021)? *PME* (%)

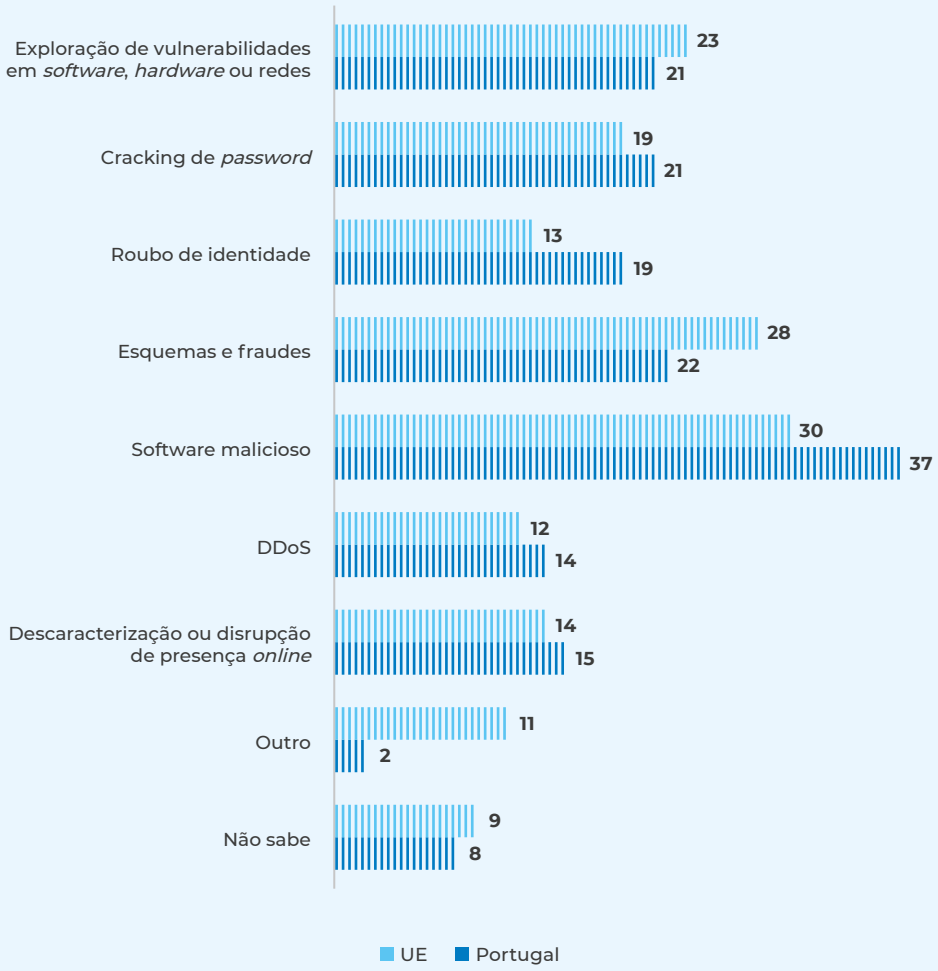


Fonte: Eurobarómetro, 2022

Um outro aspeto questionado neste inquérito é o modo como o incidente considerado mais grave ocorreu. O meio mais referido pelas PME portuguesas é o *software* malicioso, para 37%, mais 7 pp do que a média da UE. Seguem-se a exploração de vulnerabilidades, com 23%, e os esquemas e fraudes, com 22%. Este último tem mais expressão na média da UE, que chega aos 28%.

Figura 22

PENSANDO NO INCIDENTE SOFRIDO MAIS GRAVE, COMO É QUE O ATAQUE OCORREU (2021)? *PME* (%)

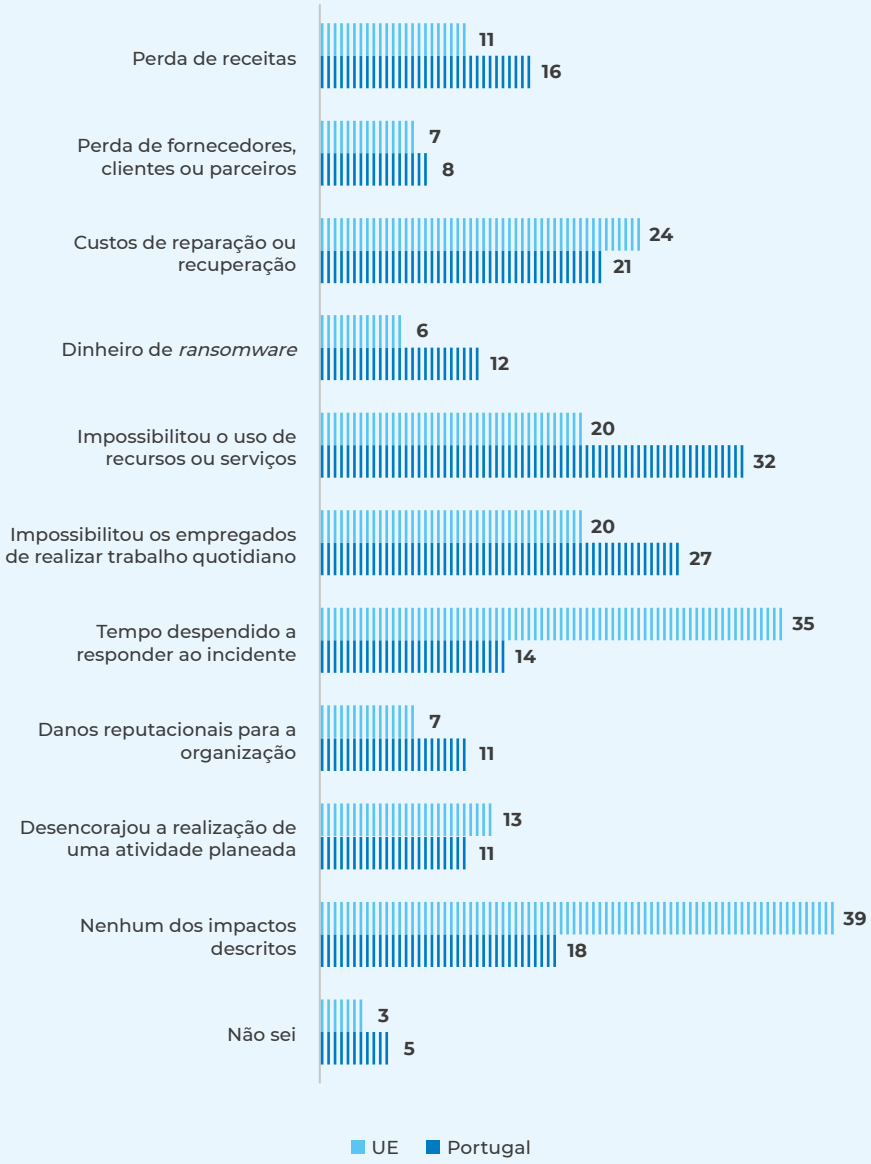


Fonte: Eurobarómetro, 2022

Quanto ao impacto do incidente mais grave, em Portugal as PME tiveram como maior consequência a impossibilidade de uso de recursos ou serviços, para 32%, enquanto na média da UE foi o tempo despendido a responder ao incidente, no valor de 35%.

Figura 23

PENSANDO AINDA NO INCIDENTE SOFRIDO MAIS GRAVE, QUE IMPACTO SOFREU O SEU NEGÓCIO (2021)?
PME (%)

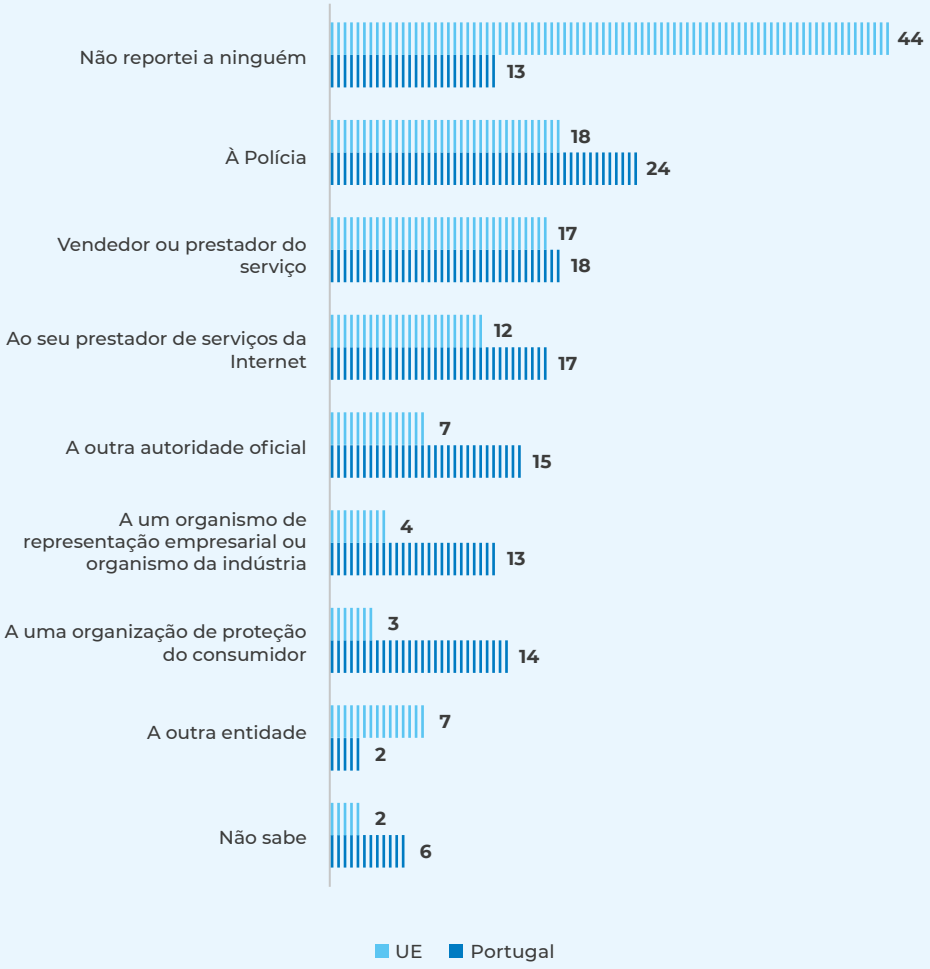


Fonte: Eurobarómetro, 2022

Há mais PME portuguesas a reportar os incidentes do que a média da UE, sendo que em Portugal 13% não reportaram e 6% não sabem, enquanto na média da UE 44% não reportaram e 2% não sabem. Portanto, em Portugal, reportaram 81% e na média da UE apenas 54%. A entidade a que mais se reportaram incidentes em Portugal (tal como na média da UE) foi a polícia, em 24% dos casos, o vendedor ou prestador do serviço, em 18%, e o prestador do serviço de Internet, em 17%.

Figura 24

A QUEM, SE ALGUÉM, REPORTOU OS INCIDENTES SOFRIDOS (2021)? (EMPRESAS QUE SOFRERAM INCIDENTES NOS ÚLTIMOS 12 MESES) *PME* (%)

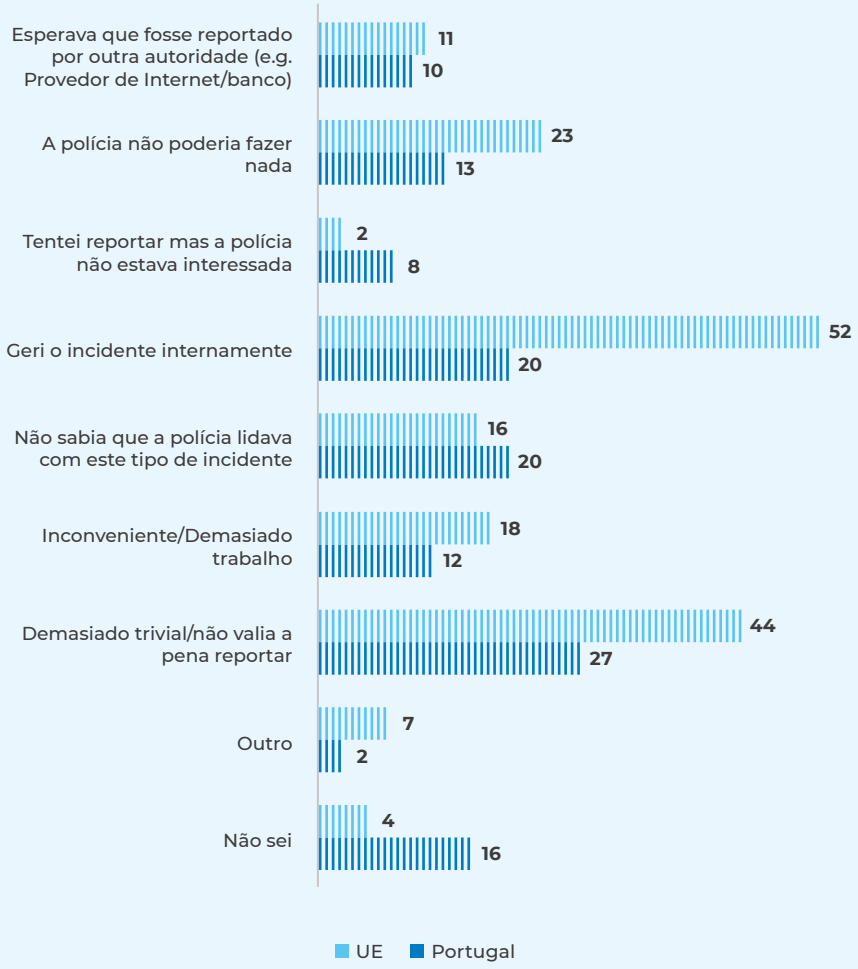


Fonte: Eurobarómetro, 2022

As respostas à questão sobre as razões que levaram os inquiridos a não reportar o incidente à polícia mostram discrepâncias relevantes entre as PME portuguesas e a média da UE. A justificação mais comum em Portugal é que o incidente era demasiado trivial e não valia a pena reportar, com 27%, ainda assim menos 17 pp do que a média da UE, com 44%. As outras duas justificações mais comuns para as PME portuguesas são o não saber que a polícia lidava com este tipo de incidente, com 20%, e o facto de o incidente ter sido gerido internamente, também com 20%. De referir que esta última é a razão mais apresentada na média da UE, com 52%.

Figura 25

PORQUE NÃO REPORTOU O INCIDENTE (OU INCIDENTES) À POLÍCIA? (EMPRESAS QUE SOFRERAM ALGUM INCIDENTE NOS ÚLTIMOS 12 MESES E NÃO REPORTARAM À POLÍCIA) *PME* (%)



Fonte: Eurobarómetro, 2022

DESTAQUES

- Em Portugal, em 2021, 67% dos inquiridos nas PME sentem-se bem informados sobre os riscos de cibercrime, menos 4 pp do que a média da UE.
- As PME portuguesas, em 2021, mostraram-se mais preocupadas com os riscos *online* do que a média da UE, em particular com o *hacking* (ou tentativas) a contas bancárias *online* (55% em Portugal e 32% na média da UE).
- Em Portugal, em 2021, 48% das PME admitem ter sofrido pelo menos um cibercrime nos últimos 12 meses, mais 20 pp do que a média da UE, com 28%.
- O método de ataque mais comum, em 2021, nos incidentes considerados mais graves foi o *software* malicioso (37% em Portugal e 30% na média da UE). Os esquemas e fraudes tiveram mais expressão na média da UE do que em Portugal (22% em Portugal e 28% na média da UE).

- O impacto mais comum para as PME portuguesas, em 2021, do incidente considerado mais grave foi a impossibilidade de uso de recursos ou serviços (32%). Na média da UE foi o tempo despendido a responder ao incidente (35%).
- As PME portuguesas, em 2021, reportaram mais incidentes do que a média da UE (81% em Portugal e 54% na média da UE). A polícia é a entidade a que mais se reporta. Quando não se reporta à polícia, em Portugal, o motivo mais comum é considerar-se demasiado trivial e que não vale a pena (27%); na média da UE, é a gestão interna do incidente (52%).

> Relação com as seguintes linhas de ação da ENSC: E1d, E2d e E2f (ver anexo).

CIBERSEGURANÇA NA ADMINISTRAÇÃO PÚBLICA

Considerando os dados publicados no *Relatório Cibersegurança em Portugal, tema Riscos e Conflitos 2022*, cerca de um terço dos incidentes registados pelo CERT.PT (equipa de resposta a incidentes de cibersegurança nacional, integrante do CNCS), em 2021, ocorreram na Administração Pública (CNCS, 2022a). Esta situação e o facto de ser um setor particularmente relevante para o funcionamento da sociedade, justificam uma análise centralizada neste domínio.

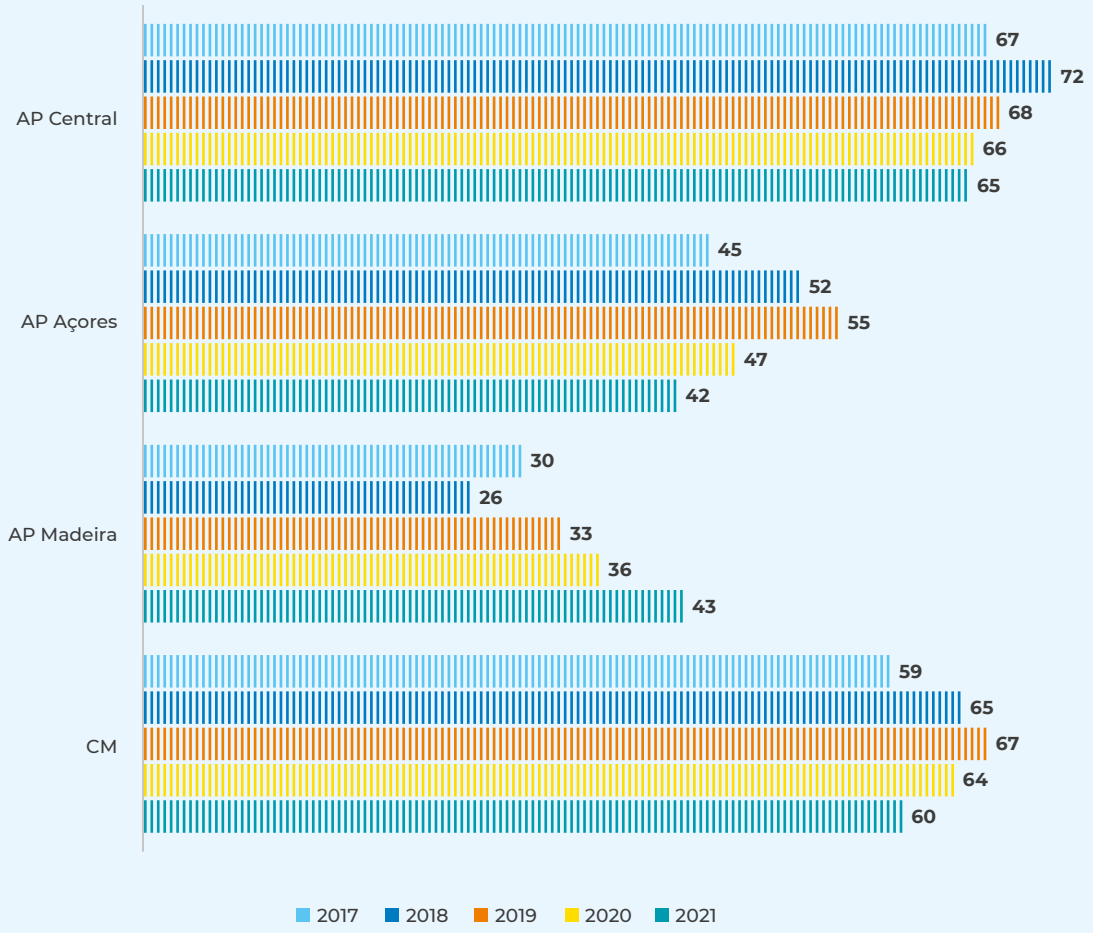
Para analisar a Administração Pública, os Inquéritos à Utilização das Tecnologias da Informação e da Comunicação (IUTIC) na Administração Pública Central e Regional e nas Câmaras Municipais, realizados pela DGEEC (2022a e 2022b), têm sido uma fonte recorrente das várias edições do presente relatório. Enquanto inquérito de resposta obrigatória pelas entidades visadas, nos termos da Lei n.º 22/2008, de 13 de maio, permite obter dados oficiais nesta matéria. O facto de haver uma secção estabilizada dedicada à cibersegurança possibilita uma análise consistente.

Verificam-se algumas tendências negativas desde pelo menos o início da pandemia da Covid-19 em 2020. A percentagem de entidades que têm definida uma estratégia para a segurança de informação tem vindo a diminuir em todos os domínios, exceto na Administração Regional da Madeira, que aumentou de 36% para 43% dos organismos, em 2021. A Administração Pública Central passou de 66% para 65%, a Administração Regional dos Açores de 47% para 42% e as Câmaras Municipais de 64% para 60%.[4]

4. Nestes inquéritos, a pergunta sobre a existência de uma Estratégia para a Segurança de Informação nos organismos da Administração Pública era realizada no módulo "Transformação Digital" até 2019. Em 2020, passou a estar inserida no módulo "Cibersegurança". Este aspeto pode ter influência em algumas respostas.

Figura 26

ENTIDADES DA ADMINISTRAÇÃO PÚBLICA QUE TÊM DEFINIDA UMA ESTRATÉGIA PARA A SEGURANÇA DE INFORMAÇÃO, EM PORTUGAL. *ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS.* (%)

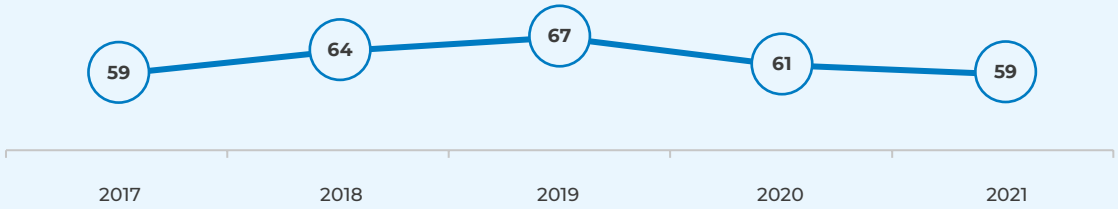


Fonte: DGEEC, 2022a e 2022b

No seu conjunto, há menos entidades da Administração Pública com uma estratégia para a segurança de informação definida. Em 2021, apenas 59% das entidades inquiridas tinham este documento, menos 2 pp do que no ano anterior, uma tendência de decrescimento que se mantém desde 2020.

Figura 27

ENTIDADES DA ADMINISTRAÇÃO PÚBLICA QUE TÊM DEFINIDA UMA ESTRATÉGIA PARA A SEGURANÇA DE INFORMAÇÃO, EM PORTUGAL. *CONJUNTO DA ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS* MUNICIPAIS (%)



Fonte: DGEEC, 2022a e 2022b

Destacando os dados relativos às Câmaras Municipais, verifica-se que a Área Metropolitana de Lisboa é a que, em 2021, tinha mais Câmaras Municipais com uma estratégia para a segurança de informação definida (89%), seguida do Norte (71%) e do Algarve (69%). A Região Autónoma do Açores (45%) e o Alentejo (42%) foram as regiões com menos Câmaras Municipais com uma estratégia deste tipo definida.

Tabela 1

PROPORÇÃO DE CÂMARAS MUNICIPAIS QUE TÊM DEFINIDA UMA ESTRATÉGIA PARA A SEGURANÇA DE INFORMAÇÃO, POR REGIÃO, EM PORTUGAL, EM 2021, *RANKING* NUTS II (%)

Área Metropolitana de Lisboa	89
Norte	71
Algarve	69
Centro	56
Região Autónoma da Madeira	55
Alentejo	45
Região Autónoma dos Açores	42

Fonte: DGEEC, 2022a e 2022b

Entre os vários tipos de entidades da Administração Pública em análise verifica-se um aumento generalizado em 2021 da aplicação de medidas de segurança das TIC, com particular destaque para a Administração Regional da Madeira, com crescimento muito significativo em algumas medidas, como sejam a identificação e autenticação do utilizador através de métodos biométricos (mais 59 pp), o uso de técnicas de "encriptação" de dados, documentos ou *emails* (mais 50 pp) e o controlo de acesso à rede do organismo (mais 25 pp). As Câmaras Municipais, diferentemente, aplicaram menos algumas destas medidas, em particular a conservação de registos para análise depois da ocorrência de incidentes de segurança (menos 7 pp).

Tabela 2

MEDIDAS DE SEGURANÇA DAS TIC UTILIZADAS NA ADMINISTRAÇÃO PÚBLICA, EM PORTUGAL. *ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS* (%)

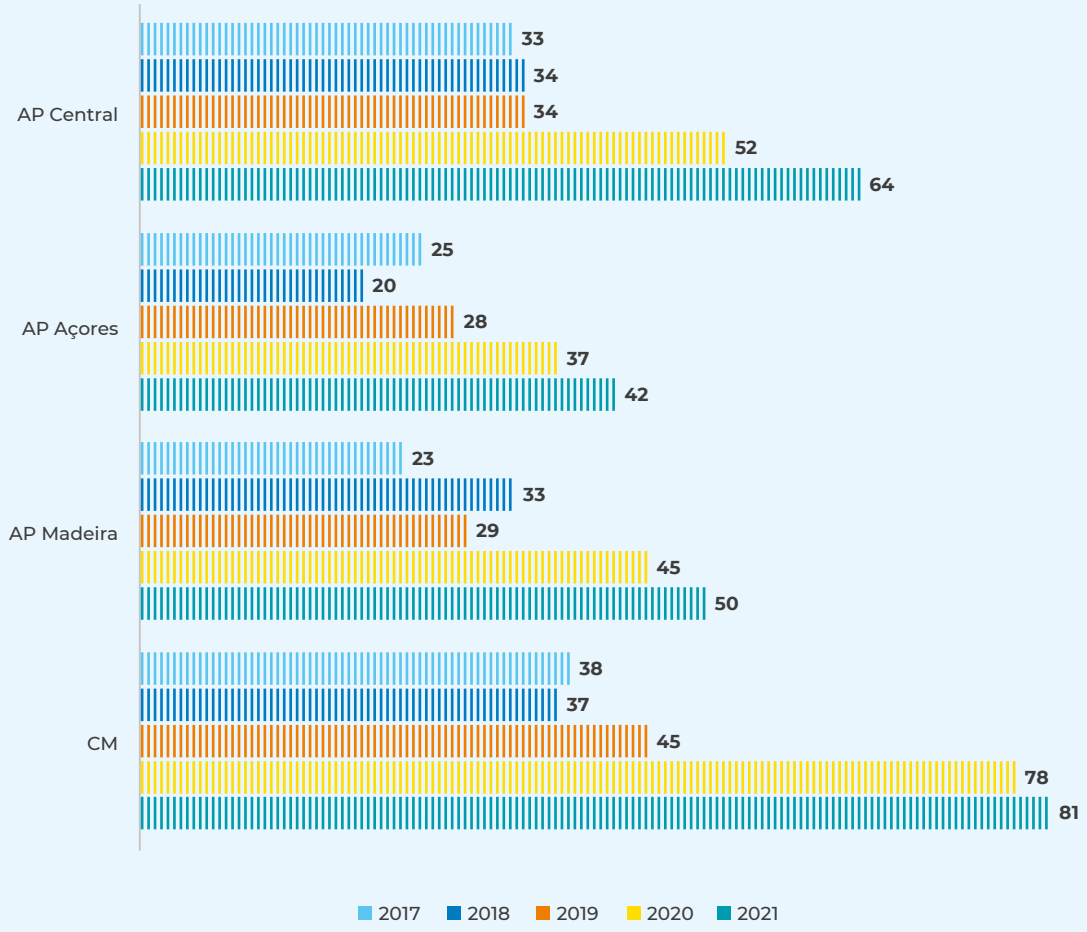
	AP Central 2021 (variação 2020 pp)	AP Açores 2021 (variação 2020 pp)	AP Madeira 2021 (variação 2020 pp)	CM 2021 (variação 2020 pp)
Atualização regular do *software*	96 (+3)	100 (=)	100 (+4)	99 (=)
Controlo de acessos à rede do Organismo	91 (+3)	96 (+2)	100 (+25)	88 (-4)
Autenticação dos utilizadores através de uma palavra-passe segura	86 (+3)	96 (-2)	100 (+9)	83 (-1)
Conservação de registos para análise depois da ocorrência de incidentes de segurança	79 (+4)	67 (-8)	79 (+17)	74 (-7)
Técnicas de encriptação de dados, documentos ou *emails*	51 (+2)	49 (+2)	98 (+50)	53 (+2)
Testes de segurança às TIC	54 (=)	47 (-12)	66 (+16)	51 (+1)
Avaliação dos riscos ligados às TIC	60 (+4)	49 (+2)	66 (+20)	48 (=)
Identificação e autenticação do utilizador através de métodos biométricos	33 (+5)	40 (-1)	96 (+59)	46 (+1)

Fonte: DGEEC, 2022a e 2022b

A necessidade elevada de reforço de competências em segurança das TIC continua a aumentar em 2021, depois de em 2020 já se ter verificado um crescimento significativo. Em 2021, 64% da Administração Pública Central afirmou ter esta necessidade, mais 12 pp do que no ano anterior. As Câmaras Municipais destacaram-se em particular, com 81%, mais 3 pp do que em 2020.

Figura 28

ENTIDADES DA ADMINISTRAÇÃO PÚBLICA QUE INDICARAM TER ELEVADA NECESSIDADE DE REFORÇO DE COMPETÊNCIAS EM SEGURANÇA DAS TIC, EM PORTUGAL. *ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS.* (%)

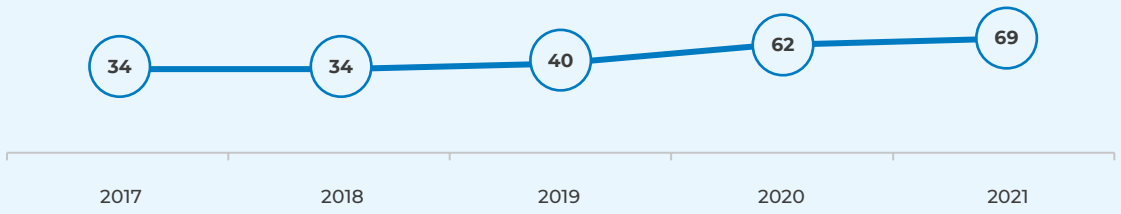


Fonte: DGEEC, 2022a e 2022b

Observando o conjunto da Administração Pública em análise, é visível a tendência crescente desde 2018 desta necessidade de reforço de competências em segurança das TIC, com particular relevância para o aumento de 2020. Em 2021, a variação registada foi de mais 7 pp do que no ano anterior, fixando-se em 69%.

Figura 29

ENTIDADES DA ADMINISTRAÇÃO PÚBLICA QUE INDICARAM TER ELEVADA NECESSIDADE DE REFORÇO DE COMPETÊNCIAS EM SEGURANÇA DAS TIC, EM PORTUGAL. *CONJUNTO DE ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS* (%)



Fonte: DGEEC, 2022a e 2022b

A região em que mais Câmaras Municipais manifestaram elevada necessidade de reforço de competências em segurança das TIC foi a Área Metropolitana de Lisboa (89%), seguindo-se o Centro (85%), o Alentejo (84%) e o Algarve (81%). Curiosamente, a Área Metropolitana de Lisboa foi igualmente a região na qual se registaram mais Câmaras Municipais com estratégias de segurança de informação definidas (também 89%), o que aparenta indicar que não haverá correlação entre os dois indicadores, algo que se aplica também à posição da Região Autónoma dos Açores, por razão inversa. Contudo, analisando o caso à luz da NUTS III, verificam-se algumas correlações negativas, analisadas no quadro destacado.

Tabela 3

PROPORÇÃO DE CÂMARAS MUNICIPAIS QUE INDICARAM TER ELEVADA NECESSIDADE DE REFORÇO DE COMPETÊNCIAS EM SEGURANÇA DAS TIC, POR REGIÃO, EM PORTUGAL, EM 2021, *RANKING* NUTS II (%)

Área Metropolitana de Lisboa	89
Centro	85
Alentejo	84
Algarve	81
Norte	80
Região Autónoma dos Açores	74
Região Autónoma da Madeira	45

Fonte: DGEEC, 2022a e 2022b

Analisando a correlação entre a existência de estratégias para a segurança de informação e a necessidade elevada de competências em segurança das TIC nas Câmaras Municipais, utilizando o coeficiente de correlação de Pearson[5], mas aplicando-o à divisão mais fina da NUTS III[6], verifica-se que existe uma correlação negativa de -0,4 (sendo -1 o máximo), isto é, quando há mais estratégias definidas há menos necessidade de competências em segurança das TIC e vice-versa. Existindo esta correlação, este valor pode, ainda assim, ser considerado fraco[7]. Esta correlação é mais forte se for tido em conta o Norte isoladamente, com -0,6; e o Centro, com -0,5. O Alentejo apenas tem uma correlação de -0,3. Portanto, estes dados indicam que em algumas regiões, mais do que noutras, as estratégias de segurança de informação tendem a ter correlação negativa com as necessidades de pessoal especializado. Em casos como o do Alentejo, de correlação muito fraca, poderia colocar-se a hipótese de a existência de uma estratégia poder ajudar a identificar mais claramente as necessidades de pessoal, mas não se verificou uma correlação positiva (cujo valor máximo seria 1).

O tipo de pessoal que realizou atividades relacionadas com a segurança das TIC na Administração Pública em análise é predominantemente do próprio organismo (entre 40% e 51%), muitas das vezes trabalhando em paralelo com fornecedores externos. As Câmaras Municipais são o tipo de organismo que mais tem este género de trabalho colaborativo (55%). A Administração Regional da Madeira tende a ter menos (9% - menos 29 pp do que no ano anterior), apresentando o valor mais alto de trabalho exclusivamente feito por colaboradores externos (39%).

Tabela 4

TIPO DE PESSOAL NA ADMINISTRAÇÃO PÚBLICA QUE REALIZOU AS ATIVIDADES RELACIONADAS COM A SEGURANÇA DAS TIC, EM PORTUGAL. *ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS* (%)

	AP Central 2021 (variação 2020 pp)	AP Açores 2021 (variação 2020 pp)	AP Madeira 2021 (variação 2020 pp)	CM 2021 (variação 2020 pp)
Pessoal do próprio Organismo (apenas)	40 (-4)	51 (-6)	46 (+10)	41 (-1)
Fornecedores externos (apenas)	17 (-2)	22 (=)	39 (+12)	2 (-2)
Pessoal do próprio Organismo e fornecedores externos	38 (-1)	16 (-6)	9 (-29)	55 (+1)

Fonte: DGEEC, 2022a e 2022b

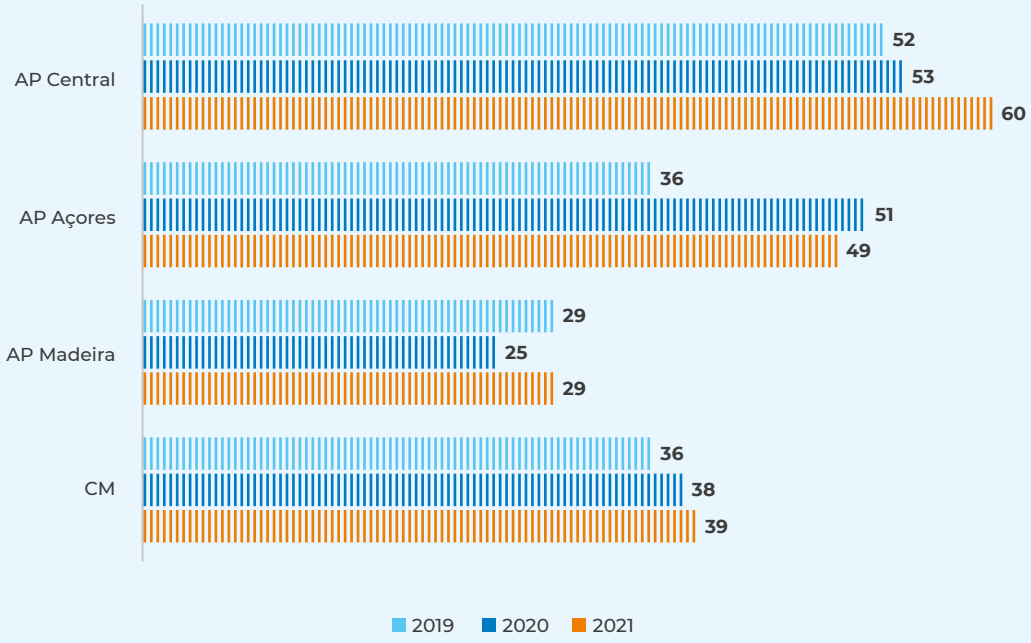
5. A correlação negativa entre duas colunas de varáveis tem expressão máxima em -1; a correlação positiva, em +1; nenhuma correlação, em 0. A correlação não significa necessariamente uma relação de causa-efeito.
(Ver: https://www.britannica.com/topic/correlation-coefficient)
6. Ver significados de NUTS: https://www.pordata.pt/O+que+sao+NUTS
7. Ver posição sobre gradação em que só a partir de 0,5 (negativo ou positivo) se considera haver uma correlação moderada: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3576830/

[consultados em 30/10/2022]

Em geral, há mais entidades da Administração Pública com recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC em 2021 do que no ano anterior. Por exemplo, a Administração Pública Central registou 60%, mais 7 pp do que em 2020. A Administração Regional dos Açores é a exceção, apresentando um ligeiro decréscimo, com 49%, menos 2 pp face ao ano anterior. As Câmaras Municipais, embora tenham melhorado a sua performance a este nível, ainda apresentam um valor relativamente baixo, de 39%, tal como a Administração Regional da Madeira, com 29%.

Figura 30

ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA QUE POSSUEM RECOMENDAÇÕES DOCUMENTADAS SOBRE MEDIDAS, PRÁTICAS OU PROCEDIMENTOS DE SEGURANÇA DAS TIC, EM PORTUGAL. *ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS* (%)



Fonte: DGEEC, 2022a e 2022b

No que diz respeito aos assuntos tratados nas recomendações referidas, assiste-se a um certo equilíbrio, sendo que o assunto que tem mais presença é o relativo ao armazenamento, proteção, acesso e processamento de dados, com 100% na Administração Regional da Madeira, e o que tem menos presença é o que diz respeito a procedimentos ou regras para prevenir ou reagir a incidentes de segurança, com 82% nas Câmaras Municipais.

Tabela 5

ASSUNTOS INSCRITOS NAS RECOMENDAÇÕES DOCUMENTADAS DA ADMINISTRAÇÃO PÚBLICA SOBRE MEDIDAS, PRÁTICAS OU PROCEDIMENTOS DE SEGURANÇA DAS TIC, EM PORTUGAL. *ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS* (%)

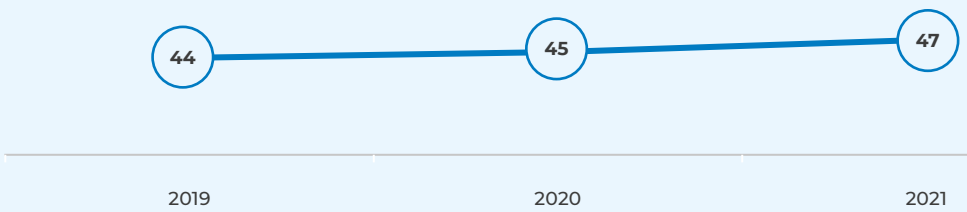
	AP Central 2021 (variação 2020 pp)	AP Açores 2021 (variação 2020 pp)	AP Madeira 2021 (variação 2020 pp)	CM 2021 (variação 2020 pp)
Gestão dos níveis de acesso às TIC	92 (-4)	89 (-11)	94 (+1)	94 (+2)
Armazenamento, proteção, acesso e processamento de dados	91 (-3)	89 (-11)	100 (=)	92 (=)
Responsabilidade, direitos e deveres no que respeita à utilização das TIC	93 (-1)	93 (+16)	94 (-6)	91 (=)
Procedimentos ou regras para prevenir ou reagir a incidentes de segurança	83 (=)	89 (+12)	88 (-5)	82 (-3)
Formação do pessoal ao serviço para uma utilização segura das TIC	92 (+1)	93 (+1)	94 (-6)	90 (-2)

Fonte: DGEEC, 2022a e 2022b

No seu conjunto, a Administração Pública tem mais recomendações deste tipo em 2021, com 47%, mais 2 pp do que em 2020. Não obstante, este valor representa menos de metade dos organismos da Administração Pública considerados.

Figura 31

ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA QUE POSSUEM RECOMENDAÇÕES DOCUMENTADAS SOBRE MEDIDAS, PRÁTICAS OU PROCEDIMENTOS DE SEGURANÇA DAS TIC, EM PORTUGAL. *CONJUNTO DA ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS* (%)

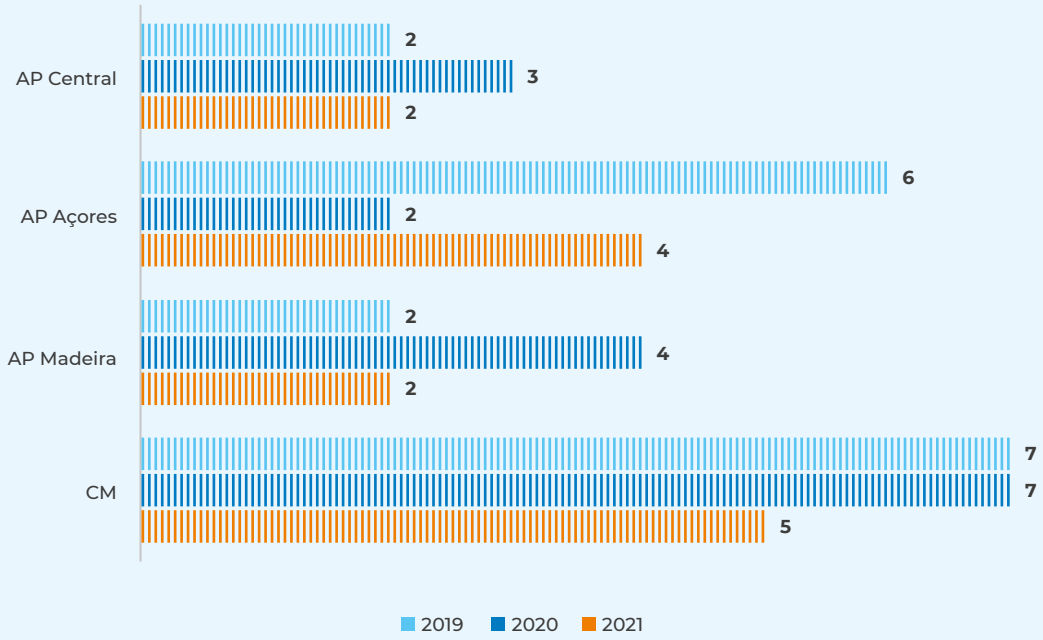


Fonte: DGEEC, 2022a e 2022b

Os dados relativos à existência de seguro contra incidentes de segurança nas TIC mostram um decréscimo na percentagem de organismos com este tipo de seguro, diminuindo um valor que já era relativamente baixo em 2020. Por exemplo, as Câmaras Municipais apresentam uma diminuição de 2 pp, para 5%, em 2021. A única exceção é a Administração Regional dos Açores, com 4%, mais 2 pp do que em 2020.

Figura 32

ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA COM SEGURO CONTRA INCIDENTES DE SEGURANÇA DAS TIC. *ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS* (%)

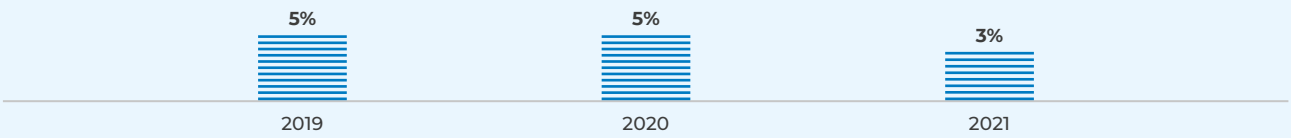


Fonte: DGEEC, 2022a e 2022b

Os dados do conjunto da Administração Pública confirmam esta perspetiva. Entre 2020 e 2021 há um decréscimo de 2 pp, de 5% para 3%, na percentagem de organismos com seguro contra incidentes de segurança das TIC.

Figura 33

ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA COM SEGURO CONTRA INCIDENTES DE SEGURANÇA DAS TIC. *CONJUNTO DA ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS* (%)



Fonte: DGEEC, 2022a e 2022b

OUTROS DADOS

Os inquéritos que servem de base à presente análise, IUTIC na Administração Pública Central e Regional, bem como nas Câmaras Municipais, da DGEEC (2022a e 2022b), apresentam outros dados de igual relevância, mas que não são considerados em profundidade neste documento devido a divergência temática. Todavia, é relevante destacar alguns desses dados.

- O tipo de aplicações de segurança das TIC mais utilizada é o *software* antivírus (e.g. 97% dos organismos da Administração Pública Central utilizam uma aplicação deste tipo);
- 94% das Câmaras Municipais utilizam uma Rede Virtual Privada (VPN);
- Enquanto apenas 22% dos organismos da Administração Pública Central indicaram que os serviços de computação em nuvem geram elevadas vantagens de segurança das TIC, entre os organismos da Administração Regional dos Açores esse indicador atinge os 67%;
- Quanto a organismos que detetaram problemas de segurança informática, verifica-se o seguinte resultado: 16% na Administração Pública Central, 2% na Administração Regional dos Açores, 7% na Administração Regional da Madeira e 11% nas Câmaras Municipais detetaram problemas deste tipo.
- Entre estes organismos que identificaram problemas de segurança informática, o tipo de problema dominante é a indisponibilidade de serviços TIC, devido a ataques externos: 47% na Administração Pública Central, nenhum na Administração Regional dos Açores, 75% na Administração Regional da Madeira e 49% nas Câmaras Municipais. Segue-se a destruição ou corrupção de dados devido a ataque ou incidentes inesperados: 26% na Administração Pública Central, 100% na Administração Regional dos Açores, 25% na Administração Regional da Madeira e 31% nas Câmaras Municipais. Por fim, a divulgação de dados confidenciais, devido a ataques de intrusão (e.g. *pharming* ou *phishing*): 28% na Administração Pública Central, nenhum na Administração Regional dos Açores e na Administração Regional da Madeira e 26% nas Câmaras Municipais.

DESTAQUES

- Há menos entidades da Administração Pública com uma estratégia para a segurança de informação definida em 2021 do que em 2020 (59% - menos 2 pp), mantendo-se a trajetória descendente iniciada em 2020.
- Aplicam-se, em geral, mais medidas de segurança das TIC na Administração Pública em 2021 do que em 2020, com particular destaque para a Administração Regional da Madeira, com crescimentos muito significativos em algumas medidas, como, por exemplo, na autenticação do utilizador através de métodos biométricos (96% - mais 59 pp).

- Verifica-se uma tendência crescente desde 2018 de entidades da Administração Pública a indicarem ter elevada necessidade de reforço de competências em segurança das TIC. Em 2021, foram 69% no conjunto em consideração, mais 7 pp do que no ano anterior.
- A Área Metropolitana de Lisboa é a região na qual há mais Câmaras Municipais, simultaneamente, com estratégias para a segurança de informação definidas (89%) e a indicarem ter elevada necessidade de reforço de competências em segurança das TIC (também 89%) – colocando-se a hipótese de as estratégias em causa ajudarem na identificação das ditas necessidades.
- Todavia, numa análise mais fina com base na NUTS III, verifica-se que existe uma correlação negativa, embora não forte, nas Câmaras Municipais, entre a existência de estratégias de segurança de informação definidas e a indicação de elevada necessidade de reforço de competências em segurança das TIC. Portanto, quanto mais estratégias definidas, menos necessidades de reforço de competências e vice-versa – colocando-se a hipótese, neste caso, de a existência de estratégias definidas mitigar as necessidades de reforço de competências nestas matérias. Esta correlação negativa é mais forte na região Norte do que no Alentejo.
- O pessoal que realiza atividades relacionadas com a segurança das TIC nas entidades da Administração Pública em análise pertence, na sua maioria, ao próprio organismo (entre 40% e 51% das atividades).
- Verifica-se a existência de mais entidades da Administração Pública com recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC em 2021 (47% - mais 2 pp do que no ano anterior), com particular destaque para o armazenamento, proteção, acesso e processamento de dados.
- Regista-se um decréscimo de entidades da Administração Pública com seguro contra incidentes de segurança das TIC, de 5% em 2020 para 3% em 2021.

> Relação com as seguintes linhas de ação da ENSC: E2d, E2e, E2f, E2l, E2m e E2r (ver anexo).

“EM 2022, VERIFICA-
-SE A EXISTÊNCIA DE 25
CURSOS SUPERIORES
DE CIBERSEGURANÇA
E SEGURANÇA DE
INFORMAÇÃO EM
PORTUGAL, MAIS TRÊS
DO QUE EM 2021”

F. SENSIBILIZAÇÃO E EDUCAÇÃO

A sensibilização e a educação em cibersegurança, quer do ponto de vista da ciber-higiene, quer em termos de especialização, são alguns dos instrumentos mais importantes para a capacitação das pessoas e, por essa via, das organizações. Neste capítulo acompanha-se, por um lado, as ações de sensibilização realizadas no país pelas organizações mais orientadas a esse tipo de atividade, com base sobretudo em inquérito realizado pelo próprio Observatório de Cibersegurança, mas também em dados do Eurobarómetro (2022) e da DGEEC (2021a e 2021b). Por outro lado, estuda-se a evolução dos cursos superiores especializados em cibersegurança e segurança de informação, bem como os números relativos aos alunos que os frequentam. Para o efeito, recorre-se a bases de dados públicas da DGEEC e da Direção-Geral de Ensino Superior (DGES) sobre cursos e alunos no ensino superior.

AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA

O CNCS procura caracterizar as ações de sensibilização em cibersegurança no país através de um inquérito anual - *Inquérito sobre a Sensibilização em Cibersegurança em Portugal* – dirigido a um conjunto de entidades selecionadas com responsabilidades de sensibilização de públicos externos nestas matérias. O inquérito não efetua uma seleção exaustiva deste tipo de entidade, apenas escolhe as consideradas mais relevantes, que tenham algum alcance e que atuem sem fins lucrativos (neste contexto)[8]. Os valores recolhidos nem sempre correspondem aos números exatos, mas sim a estimativas, nomeadamente no que diz respeito a pessoas alcançadas. Em certas situações, esses valores de alcance não se encontram disponíveis. Por isso, em geral, as estimativas apresentadas encontram-se abaixo do valor real. Todavia, esta abordagem permite considerar a distribuição das ações de sensibilização por tipologias, por públicos-alvo, por temas e por estratégias de avaliação.

8. As entidades que responderam a este inquérito foram as seguintes: Associação .PT; a Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI); o próprio CNCS e o seu Centro de Sensibilização que coordena o Centro Internet Segura; a Competitive Intelligence and Information Warfare Association (CIIWA); o Consórcio do Centro Internet Segura (que inclui DGE, IPDJ, FCT, APAV, Fundação Altice e Microsoft); a COTEC Portugal; o IAPMEI; e a Secretaria-Geral da Presidência do Conselho de Ministros.

Ao todo, considerando as ações de sensibilização em cibersegurança através de sessões presenciais e *online*, cursos *online*, redes sociais, comunicação social e outros meios, como *websites*, registaram-se cerca de 1752 ações realizadas pelas entidades em apreço, em 2021. No âmbito das sessões presenciais e *online* e dos cursos *online*, foram alcançadas cerca de 174 459 pessoas. No que diz respeito a redes sociais e outras plataformas como *websites*, registaram-se cerca de 10 015 202 visualizações de *posts* e conteúdos. No que se refere a ações na comunicação social não foi possível recolher informação sobre o respetivo alcance.

Tabela 6

AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA REALIZADAS EM PORTUGAL POR ENTIDADES COM ESSA MISSÃO SELECIONADAS, PESSOAS ALCANÇADAS PELAS MESMAS E VISUALIZAÇÕES EM REDES SOCIAIS, *WEBSITES* E OUTROS (ESTIMATIVA), 2021

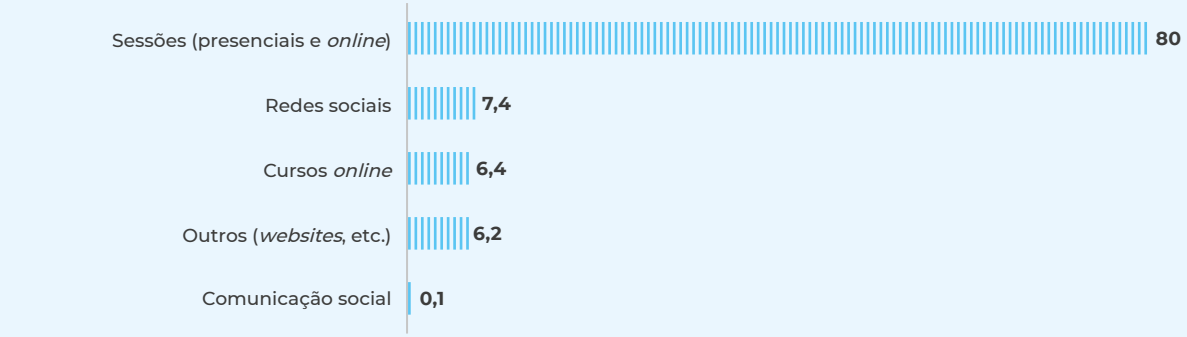
	Nº
Total de ações	1752
Pessoas alcançadas (sessões presenciais e *online* e cursos *online*)	174 459
Visualizações (redes sociais, *websites* e outros)	10 015 202

Fonte: CNCS

Uma análise ao tipo de ações realizadas por estas entidades mostra que 80% destas ações foram sessões presenciais ou *online*; 7,4% foram no âmbito de partilhas nas redes sociais; 6,4% foram cursos *online*; 6,2% dizem respeito a outos meios, como *websites*; e apenas 0,1% ocorreram na comunicação social.

Figura 34

PROPORÇÃO DE AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA POR TIPO REALIZADAS EM PORTUGAL POR ENTIDADES COM ESSA MISSÃO SELECIONADAS (ESTIMATIVA), 2021 (%)

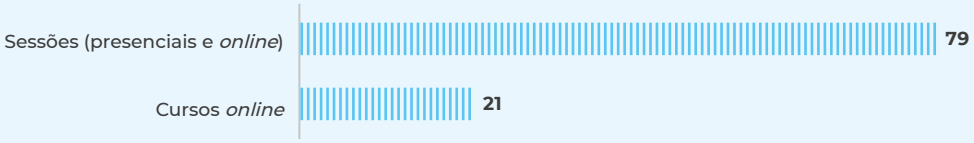


Fonte: CNCS

No âmbito das sessões e dos cursos *online* de sensibilização, verifica-se que 79% das pessoas são alcançadas através das sessões presenciais e *online* e 21% dos cursos *online*. Considerando que as sessões correspondem a 80% do total de ações e os cursos apenas a 6,4% (se forem consideradas apenas as sessões e os cursos *online*, que contabilizam o alcance de pessoas, o valor é de 93% para as sessões e de 7% para os cursos *online* em termo do número de ações), conclui-se que os cursos *online* são particularmente eficazes quanto ao número de pessoas alcançadas, verificação que não corresponde a uma avaliação da sua capacidade em alterar comportamentos.

Figura 35

PROPORÇÃO DE PESSOAS ALCANÇADAS NAS AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA, EM SESSÕES E CURSOS *ONLINE*, REALIZADAS EM PORTUGAL POR ENTIDADES COM ESSA MISSÃO SELECIONADAS (ESTIMATIVA), 2021 (%)*



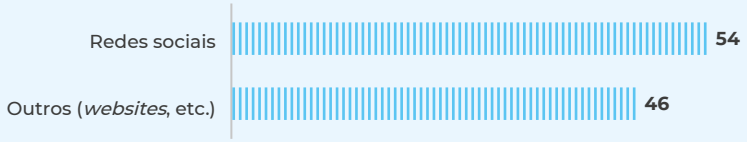
*Os dados sobre o alcance da comunicação social não se encontram disponíveis.

Fonte: CNCS

Analisando as visualizações de conteúdos em redes sociais e em *websites* e outros, constata-se que 54% ocorrem nas redes sociais e 46% em *websites* e outros. Dada a percentagem de ações em ambos - 7,4% nas redes sociais e 6,2% em *websites* e outros (se forem considerados apenas estes dois tipos de ações, que se destinam a visualizações, as redes sociais representam 53% e os *websites* e outros 47%) - estes últimos demostram ter alguma eficácia na partilha de conteúdos. Não obstante, é importante notar que muitas das visualizações em *websites* resultam de partilhas nas redes sociais.

Figura 36

PROPORÇÃO DE VISUALIZAÇÕES NAS AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA, EM REDES SOCIAIS E *WEBSITES* E OUTROS, REALIZADAS EM PORTUGAL POR ENTIDADES COM ESSA MISSÃO SELECIONADAS (ESTIMATIVA), 2021 (%)



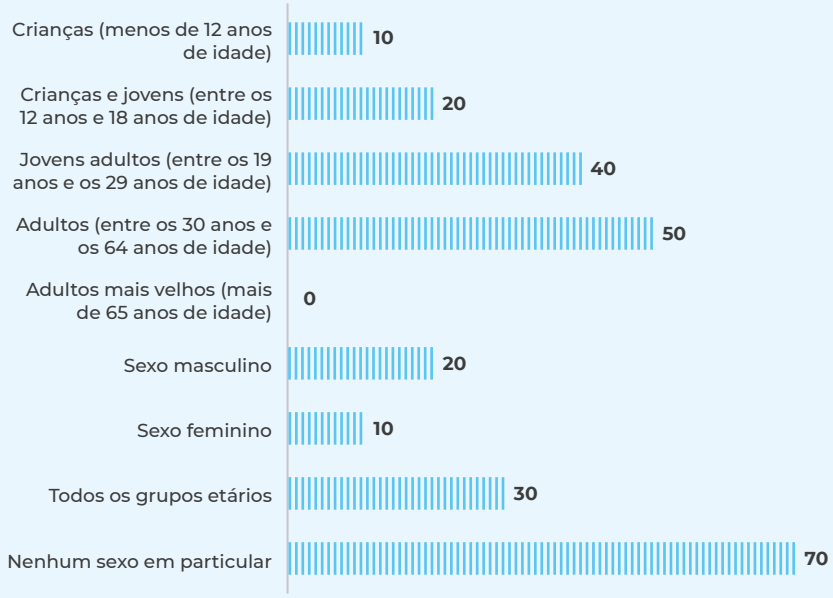
Fonte: CNCS

Uma caracterização quanto à faixa etária e ao sexo dos públicos-alvo das ações de sensibilização realizadas pelas entidades em apreço, em 2021 e 2022 (até ao 1o semestre) mostra que as faixas etárias predominantes são os adultos (30-64 anos), presentes em 50% das entidades organizadoras das ações, e os jovens adultos (19-29 anos), em 40%. É significativo que 30% das entidades se dirijam a todas as faixas etárias, o que inclui as pessoas com mais 65 anos de idade. É de notar, no entanto, que esta faixa etária não predomina como alvo em nenhuma organização. Os 30% dirigidos a todas as idades correspondem às entidades com mais ações e alcance.

Quanto ao sexo, as organizações não tendem a definir o masculino ou o feminino como alvo predominante das suas ações, pelo menos em 70% dos casos.

Figura 37

CARACTERIZAÇÃO ETÁRIA E POR SEXO DO PÚBLICO-ALVO PREDOMINANTE CONSIDERADO PELAS ENTIDADES SELECIONADAS QUE REALIZAM AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA (ESTIMATIVA), EM PORTUGAL, 2021-2022 (ATÉ 1O SEM.) (%)*



* Múltiplas respostas possíveis. De referir ainda que os 30% que atingem todas as faixas etárias correspondem às organizações com mais ações e alcance.

Fonte: CNCS

Quanto aos temas mais frequentes tratados nestas ações de sensibilização, em 2021 e 2022 (até ao 1o semestre), sobressaem as "Boas práticas genéricas de ciber-higiene", em 100% dos casos, a que se seguem os "Riscos *online* e cibercrime", em 78%, e a "Proteção de dados, privacidade e direitos", em 44%. Com relevância, surgem ainda temas como a "Gestão da cibersegurança e empresas", o "Cyberbullying", a "Desinformação", a "Prevenção de dependência e bem-estar *online*", os "Relacionamentos *online*" e os "Pagamentos e compras *online*".

Tabela 7

TEMAS TRATADOS NAS AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA REALIZADAS EM PORTUGAL POR ENTIDADES COM ESSA MISSÃO SELECIONADAS, EM 2021-2022 (ATÉ 1º SEM.) (%)*

Boas práticas genéricas de ciber-higiene	100
Riscos *online* e cibercrime	78
Proteção de dados, privacidade e direitos	44
Gestão da cibersegurança e empresas	33
Cyberbullying	33
Desinformação	33
Prevenção de dependência e bem-estar *online*	33
Relacionamentos *online*	33
Pagamentos e compras *online*	33
Discurso de ódio	22
Cidadania digital	22
Parentalidade digital	22
Fontes de informação abertas	11
Cuidados nas redes sociais	11
Digitalização e clima	11

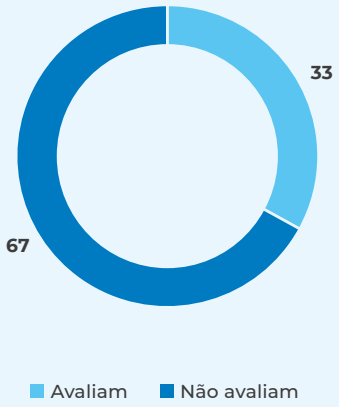
Fonte: CNCS

* Múltiplas respostas possíveis.

O último tópico deste inquérito dedica-se à eventualidade de as entidades avaliarem o impacto das suas ações de sensibilização em cibersegurança junto do seu público-alvo, sobretudo no que diz respeito à mudança positiva de comportamento – em última análise, a finalidade das ações de sensibilização. Os valores em causa continuam a ser muito reduzidos, tal como no ano anterior. Em 2021 e 2022 (até ao 1o semestre), apenas 33% das entidades realizaram algum estudo do impacto das suas ações de sensibilização (em 2020, registaram-se 25%, mas o universo era um pouco maior).

Figura 38

ENTIDADES SELECIONADAS QUE UTILIZARAM ALGUM MECANISMO DE AVALIAÇÃO DE IMPACTO DAS AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA REALIZADAS EM PORTUGAL, 2021-2022 (ATÉ 1O SEM.) (%)*



Fonte: CNCS

De referir que os tipos de metodologias mais usadas para a realização destas avaliações foram os inquéritos (67% dos casos) e a observação direta (33%). Num dos casos, realizou-se ainda um estudo mais sistemático sobre a matéria. Os inquiridos consideraram que os resultados destas avaliações mostraram impactos das ações bons (67%) ou muito bons (33%).

DESTAQUES

- Em 2021, realizaram-se pelo menos 1752 ações de sensibilização em cibersegurança no país, no âmbito das atividades de entidades com responsabilidades nessa matéria selecionadas. Estas ações atingiram cerca de 174 mil pessoas, através de sessões presenciais e *online* e cursos *online*, e permitiram mais de 10 milhões de visualizações de *posts* e conteúdos em redes sociais e *websites*.
- A maioria destas ações, em 2021, foram sessões presenciais ou *online* (80%). Seguem-se as redes sociais (7,4%), os cursos *online* (6,4%) e outros meios como *websites* (6,2%). Apenas 0,1% ocorreram nos meios de comunicação social. No entanto, verifica-se que os cursos *online* atingiram 21% das pessoas e as sessões presenciais ou *online* 79%, o que mostra alguma eficácia dos cursos *online* nesta matéria.
- As faixas etárias que predominaram como públicos-alvo em 2021 e 2022 (até ao 1ºsemestre) foram os adultos (30-64 anos), com 50%, e os jovens adultos (19-29 anos), com 40%. Contudo, as entidades com mais ações realizadas e mais alcance dirigiram-se a todas as faixas etárias, com 30%. As ações, em geral, não privilegiaram um sexo em particular.

- Os temas mais comuns nestas ações de sensibilização, em 2021 e 2022 (até ao 1o semestre), foram as "Boas práticas genéricas de ciber-higiene" (100% dos casos), os "Riscos *online* e cibercrime" (78%) e a "Proteção de dados, privacidade e direitos" (44%).
- Apenas 33% das entidades que realizaram ações de sensibilização em cibersegurança em 2021 e 2022 (até ao 1o semestre) analisaram os impactos das mesmas no comportamento dos públicos-alvo.

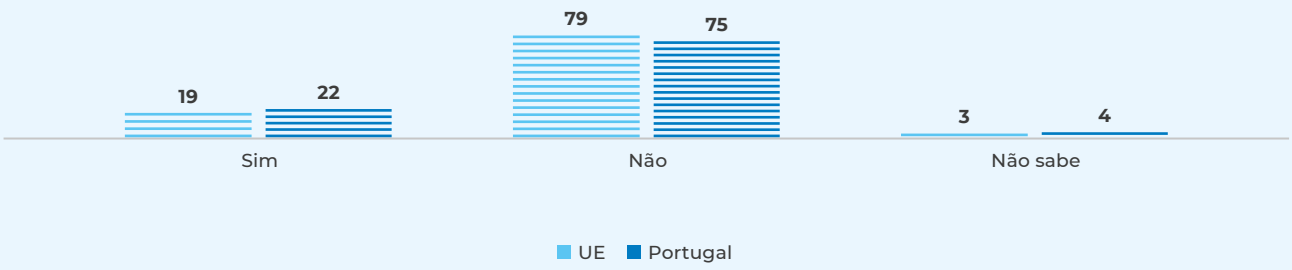
> Relação com as seguintes linhas de ação da ENSC: E2d, E3e, E2f, E2h, E2l e E2r (ver anexo).

SENSIBILIZAÇÃO NAS PME E NA ADMINISTRAÇÃO PÚBLICA

Retomando a análise do Flash Eurobarómetro 496, sobre *PME* e *Cibercrime* (Eurobarómetro, 2022), verifica-se que, no que diz respeito à sensibilização nas PME portuguesas, apenas 22% proporcionou aos seus funcionários, em 2021, qualquer tipo de ação de formação ou de consciencialização sobre os riscos do cibercrime, ainda assim acima da média da UE, que é de 19%.

Figura 39

NOS ÚLTIMOS 12 MESES, A SUA EMPRESA PROPORCIONOU AOS FUNCIONÁRIOS QUALQUER TIPO DE AÇÃO DE FORMAÇÃO OU DE CONSCIENCIALIZAÇÃO SOBRE OS RISCOS DO CIBERCRIME (2021)? *PME* (%)



Fonte: Eurobarómetro, 2022

Considerando outro inquérito já analisado, o IUTIC na Administração Pública Central, Regional e nas Câmaras Municipais (DGEEC 2022a e 2022b), no que diz respeito ao tema da sensibilização, verifica-se um aumento no tipo de ações de formação voluntária ou informação interna disponível, em 2021, em particular na Administração Pública Central (74% - mais 6 pp) e na Administração Regional da Madeira (68% - mais 9 pp). Quanto às ações de formação obrigatória e/ou consulta obrigatória de informação, regista-se um crescimento de 4 pp em quase todos os tipos de organizações, exceto nas da Administração Regional da Madeira, com 4 pp de decréscimo.

Tabela 8

TIPO DE AÇÃO EFETUADA JUNTO DO PESSOAL AO SERVIÇO PARA CONSCIENCIALIZAÇÃO DAS SUAS OBRIGAÇÕES EM MATÉRIA DE SEGURANÇA DAS TIC, EM PORTUGAL. *ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS* (%)

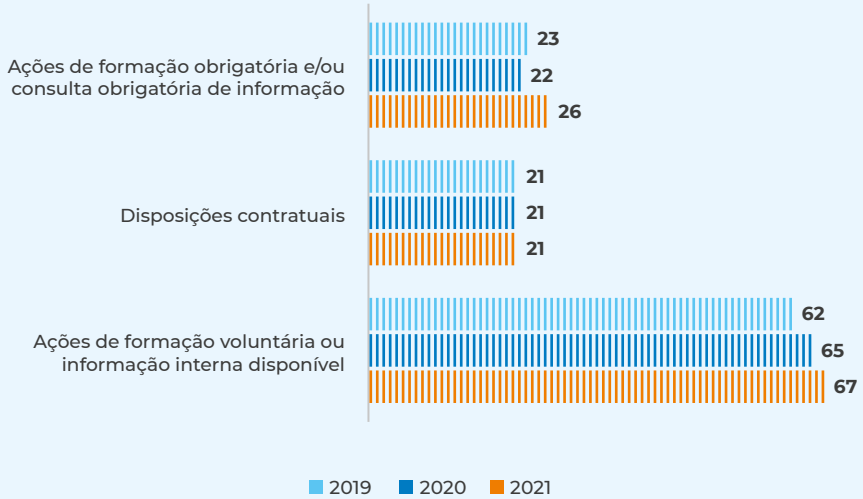
	AP Central 2021 (variação 2020 pp)	AP Açores 2021 (variação 2020 pp)	AP Madeira 2021 (variação 2020 pp)	CM 2021 (variação 2020 pp)
Ações de formação voluntária ou informação interna disponível	74 (+6)	69 (+4)	68 (+9)	61 (-1)
Disposições contratuais	24 (-1)	18 (+4)	9 (=)	21 (+1)
Ações de formação obrigatória e/ou consulta obrigatória de informação	30 (+4)	20 (+4)	23 (-4)	23 (+4)

FONTE: DGEEC 2022a e 2022b

Considerando o conjunto das entidades da Administração Pública em análise, em 2021, constata-se um crescimento de 4 pp, de 22% para 26%, na percentagem de entidades que prestaram ações de formação obrigatória e/ou consulta obrigatória de informação. Verifica-se ainda um aumento de 2 pp, de 65% para 67%, de entidades a realizar ações de formação voluntária ou a ter informação interna disponível. Como se pode verificar, as ações voluntárias predominam em comparação com as ações obrigatórias ou as disposições contratuais.

Figura 40

TIPO DE AÇÃO EFETUADA JUNTO DO PESSOAL AO SERVIÇO PARA CONSCIENCIALIZAÇÃO DAS SUAS OBRIGAÇÕES EM MATÉRIA DE SEGURANÇA DAS TIC, EM PORTUGAL. *CONJUNTO DAS ENTIDADES DA ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS* (%)



Fonte: DGEEC, 2022a e 2022b

DESTAQUES

- Apenas 22% das PME portuguesas realizou qualquer tipo de ação de formação ou de consciencialização, dirigida aos seus funcionários, sobre os riscos do cibercrime, nos últimos 12 meses, em 2021. A média da UE é de 19%.
- Na Administração Pública, no ano de 2021, a maioria das ações de formação dos funcionários para a consciencialização das suas obrigações em matéria de segurança das TIC foi voluntária, em 67% dos organismos; em apenas 26% foram obrigatórias. Todavia, ambos os tipos de ações aumentaram na Administração Pública em relação a 2020: 2 pp (voluntárias) e 4 pp (obrigatórias).

> Relação com as seguintes linhas de ação da ENSC: E2d, E2f, E2l e E2r (ver anexo).

CURSOS DO ENSINO SUPERIOR EM CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO

O ensino superior em Portugal oferece alguns cursos especializados na área da cibersegurança e segurança de informação. O presente relatório tem acompanhado esta matéria recorrendo aos registos da DGES. Em 2022, verifica-se a existência de 25 cursos superiores de cibersegurança e segurança de informação em Portugal, mais três do que em 2021. Estas três novas formações são cursos TESP.

É importante referir que esta contabilização é feita apenas relativamente aos cursos expressamente destas áreas. Não se consideram outros cursos, de informática e afins, por exemplo, que podem tratar a matéria da cibersegurança no seu currículo, embora não sejam especializados na mesma. Destes cursos saem muito profissionais de cibersegurança (para um estudo do Observatório de Cibersegurança sobre esses cursos, consultar CNCS, 2022b).

Tabela 9

CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO REGISTADOS NA DGES, EM PORTUGAL, 2022

Formação	Tipo/Grau	Instituição
Cibersegurança	TESP	Instituto Politécnico da Guarda - Escola Superior de Tecnologia e Gestão
Cibersegurança	TESP	Instituto Politécnico da Lusofonia - Escola Superior de Engenharia e Tecnologias
Cibersegurança	TESP	Instituto Politécnico de Bragança - Escola Superior de Tecnologia e de Gestão de Bragança
Cibersegurança	TESP	Instituto Politécnico Jean Piaget do Sul - Escola Superior de Tecnologia e Gestão Jean Piaget
Cibersegurança	TESP	Instituto Superior de Tecnologias Avançadas de Lisboa
Cibersegurança (NOVO)	TESP	Universidade de Aveiro - Escola Superior de Tecnologia e Gestão de Águeda
Cibersegurança e Redes informáticas	TESP	Instituto Politécnico de Leiria
Cibersegurança, Redes e Sistemas Informáticos	TESP	Instituto Politécnico do Porto - Escola Superior de Tecnologia e Gestão
Programação Ágil e Segurança de Sistemas de Informação	TESP	Instituto Politécnico de Portalegre - Escola Superior de Tecnologia e Gestão
Redes e Segurança Informática	TESP	Instituto Politécnico do Cávado e do Ave - Escola Técnica Superior
Segurança e Proteção de Dados para Sistemas de Informação	TESP	Instituto Politécnico do Cávado e do Ave - Escola Técnica Superior
Cibersegurança e Telecomunicações (NOVO)	TESP	Instituto Politécnico de Viseu - Escola Superior de Tecnologia e Gestão de Lamego
Tecnologias Militares de Segurança – Transmissões, Informática e Eletrónica (NOVO)	TESP	Instituto Universitário Militar - Unidade Politécnica Militar
Segurança Informática em Redes de Computadores	Licenciatura	Instituto Politécnico do Porto - Escola Superior de Tecnologia e Gestão
Cibersegurança	Mestrado	Instituto Politécnico de Viana do Castelo - Escola Superior de Tecnologia e Gestão
Cibersegurança	Mestrado	Universidade de Aveiro
Cibersegurança e Auditoria de Sistemas Informáticos	Mestrado	Instituto Superior Politécnico Gaya - Escola Superior de Ciência e Tecnologia
Cibersegurança e Informática Forense	Mestrado	Instituto Politécnico de Leiria - Escola Superior de Tecnologia e Gestão
Engenharia de Segurança Informática	Mestrado	Instituto Politécnico de Beja - Escola Superior de Tecnologia e de Gestão
Segurança de Informação e Direito no Ciberespaço	Mestrado	Universidade de Lisboa - Faculdade de Direito e Instituto Superior Técnico; com Instituto Universitário Militar - Escola Naval
Segurança Informática	Mestrado	Universidade de Coimbra - Faculdade de Ciências e Tecnologia
Segurança Informática	Mestrado	Universidade de Lisboa - Faculdade de Ciências
Segurança Informática	Mestrado	Universidade do Porto - Faculdade de Ciências
Tecnologias da Informação, Comunicação e Multimédia, área de especialização: Informática e Segurança da Informação*	Mestrado	Universidade da Maia
Segurança de Informação	Doutoramento	Universidade de Lisboa - Instituto Superior Técnico

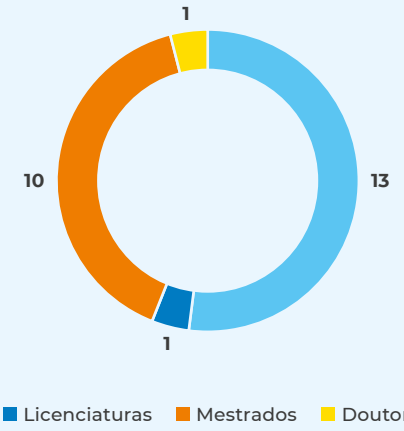
* Este mestrado já existia no ano letivo anterior, mas esta área de especialização não se apresentava identificada.

FONTE: DGES (recolha CNCS)

É notória a existência de uma discrepância em termos de volume de cursos se forem comparados os tipos/graus. Existe apenas uma licenciatura e um doutoramento, mas há 13 TESP e 10 mestrados.

Figura 41

CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL REGISTADOS NA DGES, POR TIPO/GRAU, EM 2022

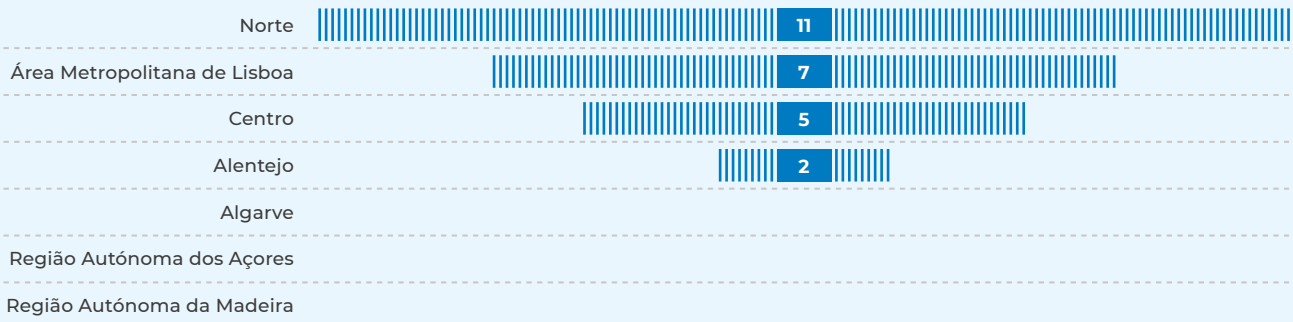


Fonte: DGES (recolha CNCS)

A distribuição geográfica destes cursos também é desequilibrada: 11 estão localizados no Norte (44%), 7 na Área Metropolitana de Lisboa (28%), 5 no Centro (20%), 2 no Alentejo (8%) e nenhum nas restantes regiões.

Figura 42

CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL REGISTADOS NA DGES, POR REGIÃO (NUTS II), EM 2022



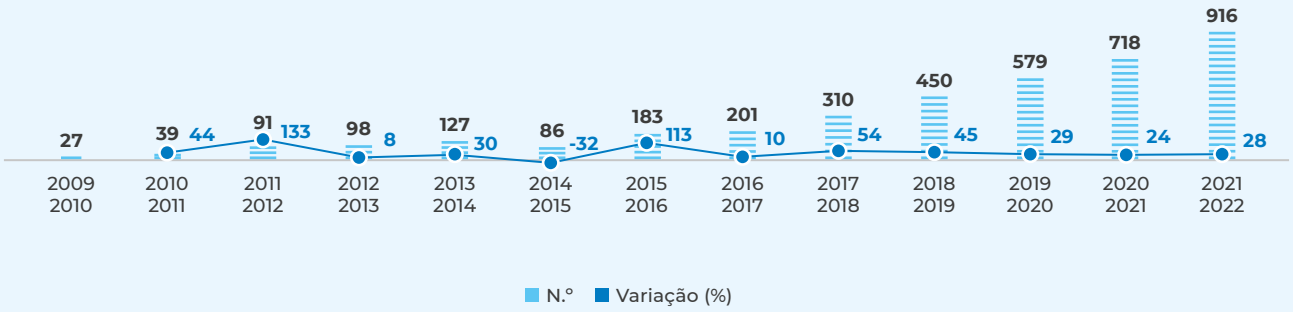
Fonte: DGES (recolha CNCS)

ALUNOS INSCRITOS E DIPLOMADOS NO ENSINO SUPERIOR DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO

O número de inscritos[9] nestes cursos continua a aumentar de ano para ano. Entre o ano letivo de 2020/2021 e o de 2021/2022 passou-se de 718 para 916 alunos inscritos, portanto, mais 198 alunos, um crescimento de 28%, uma tendência que se verifica desde o ano letivo de 2015/2016.

Figura 43

TOTAL DE ALUNOS INSCRITOS EM CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL E VARIAÇÃO ANUAL (POR ANO LETIVO)



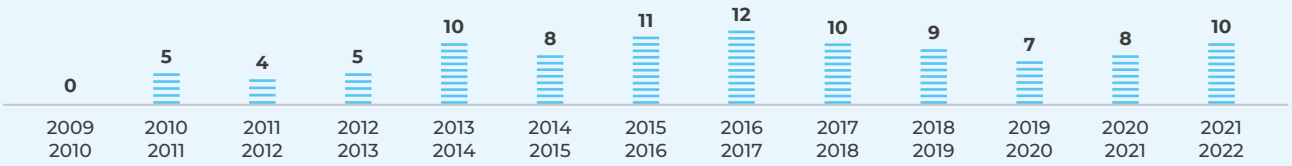
Fonte: DGEEC (recolha CNCS)

As mulheres permanecem em minoria relativamente ao número total de alunos, correspondendo a 10% dos inscritos em 2021/2022, mais 2 pp do que no ano letivo anterior. Depois de um decrescimento contínuo entre 2016/2017 e 2019/2020, regista-se deste então dois anos letivos consecutivos de aumento ligeiro deste valor.

9. "Os valores apresentados incluem os inscritos em mobilidade internacional e os inscritos em todos os cursos/ciclos de estudos ministrados em estabelecimentos de ensino superior, exceto os inscritos que estejam apenas a elaborar dissertação, trabalho de projeto ou estágio final e os inscritos em especializações que não cumpram, cumulativamente, os seguintes requisitos: 60 ECTS , 300 horas letivas de contacto distribuídas por 2 semestres letivos e avaliação final." (DGEEC)

Figura 44

PERCENTAGEM DE MULHERES INSCRITAS EM CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL (POR ANO LETIVO)

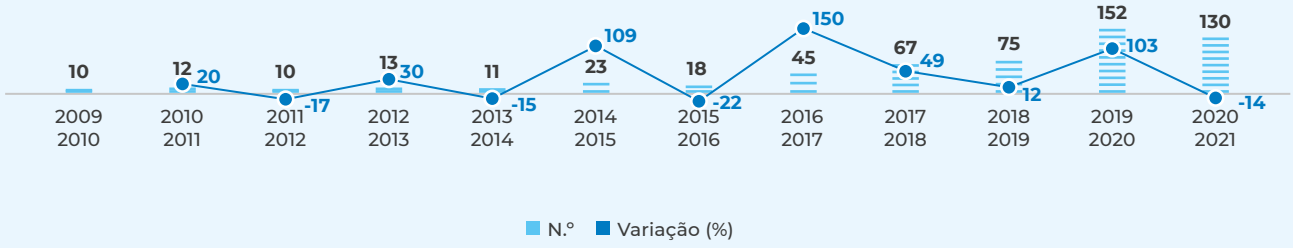


Fonte: DGEEC (recolha CNCS)

O número de diplomados nos cursos em análise não acompanhou a subida no número de inscritos, tendo-se passado de 152 diplomados em 2019/2020 para 130 em 2020/2021, menos 22, isto é, uma redução de 14%.

Figura 45

TOTAL DE ALUNOS DIPLOMADOS EM CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL E VARIAÇÃO ANUAL (POR ANO LETIVO)



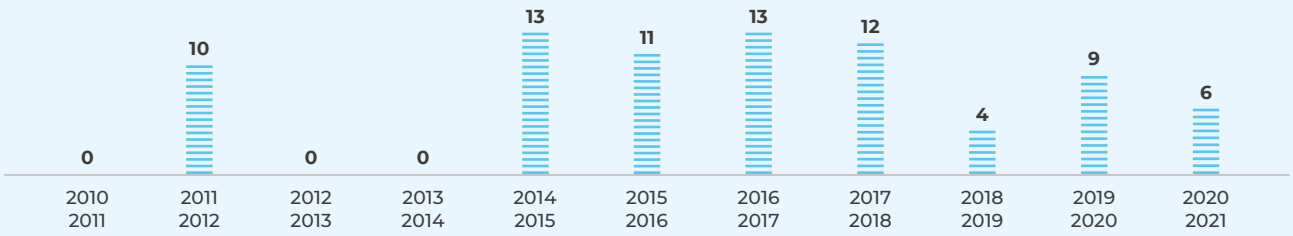
Fonte: DGEEC (recolha CNCS)

Ao contrário do ano letivo anterior, em que houve um aumento de 5 pp, em 2020/2021 verificou-se um decréscimo de 3 pp, de 9% para 6%, na proporção de mulheres relativamente ao total de diplomados nestes cursos. Comparativamente, a percentagem de mulheres diplomadas em cursos TIC em Portugal é bastante superior, com um valor de 21,9%, em 2021, uma variação positiva em relação a 2020, ano em que se fixava em 19,8% (Pordata)[10].

10. Ver Pordata: https://www.pordata.pt/subtema/portugal/sociedade+de+informacao+e+telecomunicacoes-92 [consultado em 30/10/2022]

Figura 46

PERCENTAGEM DE MULHERES DIPLOMADAS EM CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL (POR ANO LETIVO)



Fonte: DGEEC (recolha CNCS)

DESTAQUES

- Em Portugal, há mais três cursos superiores de cibersegurança e segurança de informação em 2022 do que em 2021, sendo estes três cursos TESP. Ao todo, existem 25 cursos superiores nesta área: 13 TESP, uma licenciatura, 10 mestrados e um doutoramento.
- Existe algum desequilíbrio na distribuição regional destes cursos: 11 (44%) encontram-se no Norte, 7 (28%) na Área Metropolitana de Lisboa, 5 (20%) no Centro e 2 (8%) no Alentejo. O Algarve e as Regiões Autónomas não têm nenhum destes cursos.
- Registou-se um crescimento de 28% no número de alunos inscritos nestes cursos em 2021/2022, de 718 para 916. Em 2020/2021, por sua vez, o número de alunos diplomados decresceu 14%, de 152 para 130.
- Entre os alunos inscritos em 2021/2022, 10% são mulheres (mais 2 pp do que no ano letivo anterior). Entre os diplomados em 2020/2021, 6% são mulheres (menos 3 pp do que no ano letivo anterior).

Relação com as seguintes linhas de ação da ENSC: E2e, E2g, E2h, E2k, E2l, E2m e E2r (ver anexo).

> DESDE A PUBLICAÇÃO DO PRIMEIRO *RELATÓRIO CIBERSEGURANÇA EM PORTUGAL, TEMA SOCIEDADE*, EM 2019, QUE SE VERIFICAM ALGUMAS TENDÊNCIAS POSITIVAS NAS ATITUDES, NOS COMPORTAMENTOS, NA SENSIBILIZAÇÃO E NA EDUCAÇÃO RELATIVAMENTE À CIBERSEGURANÇA NO PAÍS

G. BRIEFING – ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO

Na edição do ano passado deste documento iniciou-se uma análise aos indicadores que se cruzam com alguns eixos e linhas de ação da ENSC aprovada pela Resolução do Conselho de Ministros n.o 92/2019, de 5 de junho. O objetivo é acompanhar possíveis impactos desta ENSC na sociedade portuguesa, com particular atenção, neste relatório, para os aspetos ligados às atitudes, comportamentos, sensibilização e educação. Deste modo, o CNCS, enquanto Autoridade Nacional de Cibersegurança, além de acompanhar a execução e a revisão do Plano de Ação que é instrumento de realização desta ENSC, contribui para a compreensão dos seus eventuais impactos.

Considerando os seis eixos que constituem a atual ENSC, o segundo eixo sobressai como aquele com o qual os indicadores trabalhados neste estudo mais se relacionam - Eixo dois: prevenção, educação e sensibilização. Neste âmbito, existem indicadores de quatro tipos. Também é possível ter em conta um indicador e respetiva tipologia no que se refere ao Eixo um: estrutura de segurança do ciberespaço. Vejamos, portanto, os resultados dos cinco tipos de indicadores estudados.

1. Indicadores relativos à sensibilização do cidadão em geral (E2d e E2f): verifica-se a existência de dados positivos no que diz respeito às preocupações (o facto de crescerem demonstra consciência por parte dos cidadãos) e ao conhecimento sobre algumas matérias (e.g., sobre *cookies*), bem como no que se refere à capacidade de agir bem (e. g., na gestão dos dados pessoais *online*). Existe um número razoável de ações de sensibilização em cibersegurança para o cidadão em geral, sobre temas universais, em que os cursos *online* revelam particular eficácia em termos de alcance. Todavia, há poucas ações de sensibilização nas PME, e na Administração Pública a maioria destas ações é voluntária; ainda que, nesta mesma Administração Pública, constate-se um crescimento no número de entidades a realizarem ações de sensibilização/formação e a divulgarem recomendações.
2. Indicadores relativos à sensibilização de grupos específicos, particularmente vulneráveis (E2e e E2h): continua a registar-se um desequilíbrio entre grupos sociodemográficos relativamente ao conhecimento e aos cuidados em termos de ciber-higiene. As pessoas com mais idade e as pessoas com menos estudos ten-

dem a demonstrar possuir menos conhecimentos e a agir de forma menos correta do que as pessoas mais novas e as pessoas com mais estudos. As ações de sensibilização em cibersegurança ainda se dirigem insuficientemente a pessoas com mais idade. Além disso, a percentagem de mulheres inscritas e diplomadas em cursos especializados em cibersegurança e segurança de informação é menor do que a percentagem de mulheres diplomadas em cursos de TIC em Portugal.

3. Indicadores relativos à introdução da matéria da cibersegurança na educação formal (E2g e E2k): o número de cursos de cibersegurança e segurança de informação e o número de inscritos nestes cursos aumentou. Contudo, o número de diplomados diminuiu.
4. Indicadores relativos à qualificação de especialistas e partilha de conhecimento especializado (E2l, E2m e E2r): ainda que existam mais cursos de cibersegurança e segurança de informação no ensino superior e algumas tendências positivas no âmbito da sensibilização em contexto de trabalho, a Administração Pública em particular manifesta ter uma crescente necessidade de competências em segurança das TIC e um decrescimento no número de organismos com uma estratégia de segurança de informação definida.
5. Indicador relativo à colaboração entre entidades na reação a incidentes (E1d): as PME portuguesas reportam mais incidentes às autoridades do que a média da UE a este respeito.

H. RECOMENDAÇÕES

Quadro 2

Aspetos mais críticos	Recomendações
Uso crescente da Internet e de serviços digitais críticos para a cibersegurança.	Manter ativas as ações de sensibilização, formação e educação em matéria de cibersegurança junto dos cidadãos em geral.
Assimetrias de sexo, etárias e de formação quanto às atitudes e comportamentos. Falta de ações de sensibilização dirigidas especificamente a adultos mais velhos.	Criar estratégias de sensibilização orientadas a grupos sociodemográficos específicos, nomeadamente adultos mais velhos (tendencialmente com formação mais baixa).
Existência de menos estratégias de segurança de informação na Administração Pública Central e Regional e Câmaras Municipais.	Continuar a promover, em particular no âmbito do acompanhamento da execução da ENSC, a criação de estratégias de segurança de informação na Administração Pública. Promover ainda a adoção do Quadro Nacional de Referência para a Cibersegurança.
Falta de pessoal especializado em segurança das TIC na Administração Pública Central e Regional e Câmaras Municipais.	Promover a formação, a reconversão e/ou a contratação de pessoal no sentido de uma maior especialização em segurança das TIC.
Insuficiente avaliação dos resultados das ações de sensibilização no comportamento dos cidadãos.	Promover o estudo dos resultados das ações de sensibilização no comportamento dos públicos-alvo, utilizando metodologias variadas e não confundindo este tipo de estudo com a avaliação da qualidade.
Pouca formação e sensibilização nas PME e pouca sensibilização obrigatória na Administração Pública.	Promover junto das lideranças das PME (nomeadamente porque reconhecem ser mais vítimas de cibercrimes do que a média da UE) e da Administração Pública a necessidade de sensibilizar os colaboradores relativamente às ameaças que implicam o fator humano, em modelo obrigatório. Promover ainda a adoção do Quadro Nacional de Referência para a Cibersegurança.
Baixa percentagem de mulheres inscritas e diplomadas nos cursos de cibersegurança e segurança de informação.	Promover as profissões ligadas à cibersegurança junto do público feminino, nas escolas e nas esferas profissionais de reconversão e habilitação profissional.

Recursos de capacitação do CNCS: 4 MOOCs (Cidadão Ciberseguro, Cidadão Ciberinformado, Consumidor Ciberseguro e Cidadão Cibersocial), C-Academy, Centro Internet Segura, documentos de boas práticas, Recomendações Técnicas, Quadro Nacional de Referência para a Cibersegurança, Quadro de Avaliação de Capacidades de Cibersegurança, Web-check, Referencial de Competências em Cibersegurança, Exercício Nacional de Cibersegurança. **Consultar *website* do CNCS para aceder a estes e outros recursos:** www.cncs.gov.pt

I. NOTAS CONCLUSIVAS

Desde a publicação do primeiro *Relatório Cibersegurança em Portugal, tema Sociedade*, em 2019, que se verificam algumas tendências positivas nas atitudes, nos comportamentos, na sensibilização e na educação relativamente à cibersegurança no país. A visão integrada que se pretende neste documento permite não só identificar áreas que podem exigir mais investimento, como também ajudar na definição de estratégias, nomeadamente a ENSC. Nem sempre a variedade de dados disponível (conseguida, por exemplo, em 2020) permite uma análise tão transversal e contínua como desejável. Contudo, é notória a existência de indicadores positivos em algumas boas práticas e no que se refere à sensibilização e educação. Outros indicadores mostram tendências negativas nos últimos anos de pandemia.

Cada vez menos o ciberespaço pode ser considerado um domínio paralelo ou complementar. É um "espaço" onde muitas das interações sociais e económicas se realizam, por vezes em exclusivo. A literacia digital, enquanto competência essencial, deve incluir a cibersegurança como tema nas aprendizagens básicas, quer formais, quer informais, de modo a preparar os cidadãos para as atividades no ciberespaço. O desenvolvimento de um tema ligado à cibersegurança no Referencial de Educação Para a Segurança, a Defesa e a Paz, utilizado na área de Educação para a Cidadania, numa parceria entre a Direção-Geral da Educação (DGE), o Instituto da Defesa Nacional (IDN) e o CNCS, aplicável voluntariamente desde o ensino básico ao secundário, é um exemplo de integração da cibersegurança no ensino formal.

Para lá das competências transversais em ciber-higiene, a complexidade e o nível de desenvolvimento das tecnologias digitais exigem profissionais altamente qualificados. Esta qualificação não é necessariamente linear. Os percursos curriculares são por vezes multifacetados. Por isso, a transversalidade temática da cibersegurança também pode ser promovida entre as várias áreas científicas e disciplinares. O presente relatório mostra uma evolução em geral positiva no número de cursos e alunos especializados nesta área. Além disso, o CNCS desenvolveu um Referencial de Competências em Cibersegurança que pode ser útil para a definição de perfis académicos e profissionais nesta matéria (CNCS, 2022c).

A ciber-higiene, para o cidadão em geral, e a cibersegurança especializada, para os profissionais, são essenciais para a capacitação humana. A evolução positiva nesta matéria não pode, contudo, ignorar a necessidade de fazer acompanhar de normas e obrigações as mudanças culturais. Uma ainda maior formalização da cibersegurança na educação poderá ser um passo nesse sentido.

J. NOTAS METODOLÓGICAS

O *Relatório Cibersegurança em Portugal, tema Sociedade 2022* desenvolveu-se com base na recolha de dados disponíveis, na sistematização de dados que não se encontravam analisados e na produção de outros que não existiam, mediante inquérito, por exemplo.

No capítulo respeitante ao Ambiente Sociotécnico, utilizaram-se dados sobretudo do Eurostat, a saber: *Individuals – internet use, Individuals – internet activities e Internet purchases by individuals*, realizados no âmbito do IUTIC às famílias 2021, entre 9 de junho e 3 de setembro de 2021, tendo sido questionados em Portugal 6185 indivíduos com idades entre os 16 e os 74 anos (Eurostat, 2021a, 2021c e 2021d); e *Type of connections to the internet*, integrado no IUTIC às empresas 2021, realizado entre 15 de fevereiro e 31 de julho de 2021, a 8083 empresas em Portugal (Eurostat, 2021b). Os dados da ANACOM (2022), por sua vez, são recolhidos pela mesma trimestralmente junto dos prestadores de comunicações eletrónicas.

Os valores apresentados relativamente às pesquisas no motor de busca Google foram recolhidos na plataforma Google Trends no dia 14 de outubro de 2022.

No âmbito das Atitudes e Comportamentos, recorreu-se a dados do Flash Eurobarómetro 496, dedicado ao tema *PME e Cibercrime*, no âmbito do qual se realizou um inquérito, entre 26 de novembro e 17 de dezembro de 2021, a PME da UE, tendo sido realizadas 511 entrevistas em Portugal (Eurobarómetro, 2022). Os dados do inquérito do Eurostat relativos a *Privacy and protection of personal data* e *Internet purchases by individuals [+ perceived barriers + problems encountered]* foram recolhidos no âmbito do IUTIC às famílias 2021, já referido (Eurostat, 2021d e 2021e). No que diz respeito aos IUTIC na Administração Pública Central e Regional e Câmaras Municipais, realizados pela DGEEC (2022a e 2022b), dirigiram-se à totalidade do universo em causa e foram aplicados entre setembro de 2021 e fevereiro 2022 a 273 (99%) organismos da Administração Pública Central, 55 (100%) da Administração Pública Regional dos Açores e 56 (100%) da Madeira, bem como a 308 (100%) Câmaras Municipais. Segundo a DGEEC, "a população-alvo é constituída pelos organismos da Administração Central e Regional (exceto fundos de segurança social), constituídos em pessoas coletivas, com exceção das empresas públicas sob controlo de uma unidade da Administração Central ou Regional, Universidades, Estabelecimentos de ensino, Estabelecimentos hospitalares e estruturas temporárias. A base de inquirição é da responsabilidade do Instituto Nacional de Estatística (INE), tendo por referência o ficheiro das Contas Nacionais. Este ficheiro é atualizado anualmente, pelo que os organismos inquiridos no âmbito do IUTICAP podem variar de ano para ano".

No que se refere ao capítulo Sensibilização e Educação, os dados relativos às ações de sensibilização em cibersegurança realizados por entidades com essa missão foram recolhidos através do *Inquérito sobre a Sensibilização em Cibersegurança em Portugal 2021/2022*, realizado pelo CNCS entre 26 de outubro e 15 de novembro de 2022, obtendo-se a resposta de nove entidades, representando na realidade 13 (o Consórcio do Centro Internet Segura representa cinco). Os dados sobre as ações de sensibilização junto de colaboradores das PME e da Administração Pública resultam do Flash Eurobarómetro 496 (Eurobarómetro, 2022) e dos IUTIC na Administração Pública Central e Regional e Câmaras Municipais, da DGEEC (2022a e 2022b), já mencionados. As informações produzidas sobre os cursos superiores e os alunos inscritos e diplomados são recolhidas pelo CNCS, para análise, nos *websites* da DGES e da DGEEC.

Para mais informações acerca dos aspetos metodológicos do presente relatório, consultar as fontes mencionadas nas referências bibliográficas ou contactar o CNCS.

K. ENTIDADES PARCEIRAS DO ÂMBITO DA LINHA DE OBSERVAÇÃO SOCIEDADE

- **AP2SI** - Associação Portuguesa para a Promoção da Segurança da Informação
- **Associação .PT**
- **CIIWA** - Competitive Intelligence and Information Warfare Association
- **Consórcio Centro Internet Segura**
- **COTEC** Portugal - Associação Empresarial para a Inovação
- **DGE** - Direção-Geral da Educação
- **DGEEC** - Direção-Geral de Estatísticas da Educação e Ciência
- **IAPMEI** - Agência para a Competitividade e Inovação, I.P.
- **IPDJ** - Instituto Português do Desporto e Juventude
- **Secretaria-Geral da Presidência do Conselho de Ministros**

L. O OBSERVATÓRIO DE CIBERSEGURANÇA DO CNCS

Um Observatório, por definição, analisa uma dada realidade com o objetivo de a tornar mais compreensível e, portanto, a ação em relação à mesma mais consciente e estratégica. O Observatório de Cibersegurança visa observar o fenómeno da cibersegurança em Portugal, nas suas mais variadas componentes, de modo a informar as partes interessadas e a suportar a definição de políticas públicas. Com uma visão multidisciplinar, o Observatório de Cibersegurança sistematiza informação disponível ou promove a sua recolha nos domínios da Sociedade, Economia, Políticas Públicas, Ética e Direito, Riscos e Conflitos, bem como Inovação e Tecnologias Futuras.

Como modelo de governança, o Observatório de Cibersegurança funciona em duas esferas:

CONSELHO CONSULTIVO

Constituído por académicos de cada uma das áreas científicas das Linhas de Observação, tem como missão avaliar, propor e discutir indicadores, pesquisas e produtos, bem como sugerir a elaboração de documentos e a realização de encontros. O Conselho Consultivo deve trabalhar como conjunto, mas, eventualmente, poderá ser dividido em grupos de trabalho setoriais. O Conselho Consultivo do Observatório de Cibersegurança: https://www.cncs.gov.pt/pt/observatorio/#conselho

PARCEIROS

Numa lógica de envolvimento da comunidade, pretende criar-se relações no âmbito do Observatório de Cibersegurança com entidades da sociedade civil, com as quais se procura contactar e estabelecer parcerias. Estas entidades podem contribuir de três modos diferentes, dependendo das suas características, para o conhecimento sobre a cibersegurança em Portugal: produzindo estatísticas; desenvolvendo I&D; ou mediando a recolha de dados junto dos públicos-alvo.

> Página do Observatório de Cibersegurança do CNCS:
> https://www.cncs.gov.pt/pt/observatorio/

M. TERMOS, SIGLAS E ABREVIATURAS

Atitudes [em cibersegurança]: respeitantes às "crenças, valores, disposições mentais e emocionais dos indivíduos em relação à cibersegurança".

(adaptado de CNCS, 2019)

Ciberameaça [ameaça]: "potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização", no âmbito do ciberespaço.

(EU/IEC 27032, 2012)

Cibercrimes: "factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa." [O **cibercriminoso** é aquele que pratica estes crimes; contudo, no âmbito dos agentes de ameaças, esta designação é atribuída àquele que pratica estes crimes com intenções sobretudo económicas].

(ENSC 2019-2023 [e ENISA, *Threat Landscape* 2021])

Ciberespaço: "consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação".

(ENSC)

Ciber-higiene: "cobre várias práticas, de proteção *online* dos utilizadores e das empresas, que devem ser implementadas e desenvolvidas regularmente".

(ENISA, 2017)

Cibersegurança: "consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem".

(ENSC)

Comportamentos [em cibersegurança]: referente às "ações que os indivíduos realizam no âmbito das tecnologias digitais em termos de cibersegurança".

(adaptado de CNCS, 2019)

Sensibilização e Educação [em cibersegurança]: "ações que procuram formar os indivíduos em cibersegurança, quer no ensino formal, quer através de programas orientados ao cidadão".

(adaptado de CNCS, 2019)

Engenharia social: "ato de enganar um indivíduo no sentido de este revelar informação sensível, assim obtendo-se acesso não autorizado ou cometendo fraude, com base numa associação com este indivíduo de modo a ganhar a sua confiança".

(Grassi *et al.*, 2017)

Incidentes: "eventos com um efeito adverso real na segurança das redes e dos sistemas de informação".

(Lei no 46/2018)

Phishing [e Smishing, Vishing]: "mecanismo de elaboração de mensagens que usam técnicas de engenharia social de modo que o alvo seja ludibriado 'mordendo o isco'. Mais especificamente, os atacantes tentam enganar os recetores de *emails* ou mensagens para que estes abram anexos maliciosos, cliquem em URL inseguros, revelem as suas credenciais através de páginas de *phishing* aparentemente legítimas [*pharming*], façam transferências de dinheiro, etc." [quando esta técnica é aplicada através de SMS, dá pelo nome de *smishing*; quando o é mediante telefonema, *vishing*]

(ENISA, 2019)

Ransomware: tipo de *software* malicioso que permite que "um atacante se apodere dos ficheiros e/ou dispositivos de uma vítima, bloqueando a possibilidade de esta poder aceder-lhes.

Para a recuperação dos ficheiros, é exigido ao proprietário um resgate em criptomoedas."

(ENISA, 2019)

- **ANACOM:** Autoridade Nacional de Comunicações.
- **AP Açores:** Administração Pública Regional dos Açores.
- **APAV:** Associação Portuguesa de Apoio à Vítima.
- **AP Central:** Administração Pública Central.
- **AP Madeira:** Administração Pública Regional da Madeira.
- **AP2SI:** Associação Portuguesa para a Promoção da Segurança da Informação.
- **CERT.PT:** Equipa de Resposta a Incidentes de Segurança Informática Nacional (Lei no 46/2018) [CERT – Computer Emergency Response Team].
- **CIIWA:** Competitive Intelligence and Information Warfare Association.
- **CM:** Câmaras Municipais.
- **CNCS:** Centro Nacional de Cibersegurança.
- **COTEC [Portugal]:** Associação Empresarial para a Inovação.
- **DoS/DDoS:** Negação de Serviço/Negação de Serviço Distribuída.
- **DGE:** Direção-Geral da Educação.

- **DGEEC:** Direção-Geral de Estatísticas da Educação e Ciência.
- **DGES:** Direção-Geral de Ensino Superior.
- **DSL:** Linha Digital de Assinante [Digital Subscriber Line].
- **ENSC:** Estratégia Nacional de Segurança do Ciberespaço 2019-2023.
- **FCT:** Fundação para a Ciência e Tecnologia.
- **IAPMEI:** Agência para a Competitividade e Inovação.
- **IDN:** Instituto da Defesa Nacional.
- **INE:** Instituto Nacional de Estatística.
- **IPDJ:** Instituto Português do Desporto e Juventude.
- **MOOC:** Curso Online Aberto e Massivo [Massive Open Online Course].
- **NUTS:** Nomenclatura das Unidades Territoriais para Fins Estatísticos.
- **PME:** Pequenas e Médias Empresas.
- **pp:** pontos percentuais.
- **PT:** Portugal.
- **RDP:** Protocolo de Ambiente de Trabalho Remoto [Remote Desktop Protocol].
- **TESP:** Curso Técnico Superior Profissional.
- **TIC:** Tecnologias de Informação e Comunicação.
- **UE:** União Europeia.
- **VPN:** Rede Virtual Privada [Virtual Private Network].

N. REFERÊNCIAS PRINCIPAIS

RELATÓRIOS

[consultados a 01/11/2022]:

- ANACOM (2022) *Pandemia COVID-19 - Impacto na utilização dos serviços de comunicações em 2021* (Relatório Anual). Autoridade Nacional de Comunicações. Disponível em https://www.anacom.pt/render.jsp?contentId=1719175
- CNCS (2022a) *Relatório Cibersegurança em Portugal – Riscos & Conflitos 2022*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf
- CNCS (2022b) *Estudo Sobre o Ensino Pós-Secundário e o Ensino Superior de Cibersegurança*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/estudo-ensino-ciberseg-cncs.pdf
- CNCS (2022c) *Referencial de Competências em Cibersegurança*. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/pt/referencial-de-competencias/
- CNCS (2021a) *Relatório Cibersegurança em Portugal – Riscos & Conflitos 2021*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca--cncs.pdf
- CNCS (2021b) *Relatório Cibersegurança em Portugal – Sociedade 2021*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/relatorio-sociedade2021-observ-cncs.pdf
- CNCS (2019) *Relatório Cibersegurança em Portugal* – Sociedade 2019. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/relatrio-sociedade-2019-observatrio-de-ciberseguranа-cncs--v3-1.pdf
- ENISA (2021) *ENISA Threat Landscape 2021*. ENISA-European Union Agency for Cybersecurity. Disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
- ENISA (2019) *ENISA Threat Landscape 2018*. ENISA-European Union Agency for Cybersecurity. Disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

INQUÉRITOS

[consultados a 01/11/2022]:

- DGEEC (2022a) *Inquérito à Utilização das Tecnologias da Informação e Comunicação na Administração Pública Central e Regional* – IUTICAP 2021. Direção-Geral de Estatísticas da Educação e Ciência. Disponível em: https://www.dgeec.mec.pt/np4/12.html
- DGEEC (2022b) *Inquérito à Utilização das Tecnologias da Informação e Comunicação nas Câmaras Municipais* - IUTICCM 2021. Direção-Geral de Estatísticas da Educação e Ciência. Disponível em: https://www.dgeec.mec.pt/np4/12.html
- Eurobarómetro (2022) *Flash Eurobarómetro 496 PMEs e crime cibernético*. Eurobarómetro. Disponível em: https://europa.eu/eurobarometer/surveys/detail/2280
- Eurostat (2021a) *Individuals – internet use*. Eurostat. ISOC_CI_IFP_IU. Disponível em: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_ci_ifp_iu
- Eurostat (2021b) *Type of connections to the internet*. Eurostat: ISOC_CI_IT_EN2. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_it_en2/default/table?lang=en
- Eurostat (2021c) *Individuals – internet activities*. Eurostat. ISOC_CI_AC_I. Disponível em: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_ci_ac_i
- Eurostat (2021d) *Internet purchases by individuals [+ perceived barriers + problems encountered]*. Eurostat. ISOC_EC_IB20. Disponível em: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_ec_ib20
- Eurostat (2021e) *Privacy and protection of personal data*. Eurostat. ISOC_CISCI_PRV20. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_PRV20/bookmark/line?lang=en&bookmarkId=87227240-f5dc-43d6-af3e-5a7e6ef3a0ac

OUTROS DOCUMENTOS

[consultados a 01/11/2022]:

- ENISA (2017) *Overview of Cybersecurity and Related Terminology*. ENISA-European Union Agency for Cybersecurity. Disponível em: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology
- Grassi, P., Garcia, M. e Fenton, J. (2017) *Digital Identity Guidelines, Special Publication* (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD. Disponível em: https://doi.org/10.6028/NIST.SP.800-63-3
- Mukaka, M. M. (2012) *A guide to appropriate use of Correlation coefficient in medical research*. Malawi Medical Journal, Sep; 24(3): 69–71. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3576830/
- ISO/IEC 27032 (2012) *Information technology – Security techniques – Guidelines for cybersecurity*. International Standards Organization. Disponível em: https://www.iso.org/standard/44375.html

LEGISLAÇÃO E POLÍTICAS PÚBLICAS

(consultadas a 01/11/2022)

- Estratégia Nacional de Segurança do Ciberespaço - Resolução do Conselho de Ministros n.o 92/2019. Diário da República, Série I, n.o 108 (05-06-2019), pp. 2888 – 2895. Disponível em: https://dre.pt/dre/detalhe/resolucao-conselho-ministros/92-2019-122498962
- Regime Jurídico da Segurança do Ciberespaço - Lei n.o 46/2018. Diário da República, Série I, n.o 155 (13-08-2021), pp. 4031 – 403. Disponível em: https://dre.pt/dre/detalhe/lei/46-2018-116029384

WEBSITES

[consultados a 01/11/2022]:

- https://www.britannica.com
- www.cncs.gov.pt
- www.dgeec.mec.pt
- https://www.pordata.pt/
- trends.google.com/trends/?geo=PT

ANEXO. LINHAS DE AÇÃO DA ENSC - SOCIEDADE

Quadro 3

Linhas de Ação da ENSC, Eixo 1 e Eixo 2, articuláveis com os indicadores deste relatório		A&C*	S&E
E1d) **	Reforçar a capacidade de cibersegurança nacional tendo em vista maximizar a resiliência das Forças e Serviços de Segurança, proteção e socorro, para fazer face a incidentes ou ciberataques significativos, no âmbito das respetivas atribuições, sendo fundamental uma estreita ligação e coordenação com os diversos atores relevantes em casos de incidentes.	●	
E2d)	Criar uma sociedade mais resiliente, estimulando nos cidadãos o desenvolvimento de competências digitais, sem prejuízo de outros programas nacionais de índole congénere como é o caso, designadamente, do programa «Iniciativa Nacional Competências Digitais e.2030 – INCoDe.2030».	●	
E2e)	Criar instrumentos e reforçar as medidas de sensibilização da sociedade civil para o uso seguro e responsável das tecnologias digitais, dando particular importância à capacitação e conhecimento obtidos por crianças, adolescentes, população sénior e outros grupos de risco.	●	●
E2f)	Promover programas de capacitação em cibersegurança, robustos e transversais a todas as organizações e ao cidadão comum, permitindo que os utilizadores entendam as suas responsabilidades, usando e protegendo adequadamente as informações e os recursos que lhes são confiados.	●	●
E2g)	Reforçar as competências e conhecimentos em segurança do ciberespaço na educação, incluindo estas temáticas na estrutura curricular dos ensinos básico, secundário e superior e na formação contínua de professores.		●
E2h)	Promover a educação e literacia digital enquanto condição basilar para a confiança e utilização dos recursos digitais de uma forma consciente, informada e responsável das novas tecnologias pelas novas gerações e os grupos especialmente vulneráveis.	●	●
E2k)	Valorizar a inclusão do comportamento consciente e responsável da utilização da tecnologia enquanto parte integrante e transversal da formação académica e profissional corrente.		●
E2l)	Promover formação especializada e sensibilizar os decisores, gestores públicos e operadores de infraestruturas críticas e de entidades que fornecem serviços essenciais à sociedade, numa ótica de consciencialização e prevenção para a necessidade de salvaguardar os interesses e informação crítica nacional.		●
E2m)	Valorizar os profissionais no âmbito da segurança do ciberespaço, ampliando o número de especialistas, qualificando profissionais e envolvendo os diversos atores de toda a sociedade.		●
E2 r)	Promover programas de sensibilização específicos junto das instituições públicas e privadas, que robusteçam a vertente comportamental de segurança em ambiente digital, com base na partilha de conhecimento especializado sobre os agentes da ameaça e seus modos de atuação.		●

* A&C: atitudes e comportamentos; S&E: sensibilização e educação.
** Codificação atribuída com base no eixo em questão (E1 e E2) e na sequência pela qual surgem as linhas de ação, alinhadas com a ordem alfabética.

Observatório
de **Cibersegurança**

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

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