CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

DEZEMBRO 2023

RELATÓRIO CIBERSEGURANÇA EM PORTUGAL

SOCIEDADE 2023

5ª EDIÇÃO

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

ÍNDICE

“O COMPORTAMENTO HUMANO RELATIVAMENTE ÀS TECNOLOGIAS DIGITAIS É UM DOS FATORES MAIS DETERMINANTES PARA A SEGURANÇA DO CIBERESPAÇO.”

A. SUMÁRIO EXECUTIVO

O comportamento humano relativamente às tecnologias digitais é um dos fatores mais determinantes para a segurança do ciberespaço. Não sendo recomendável seguir simplificações que assumam o "fator humano" como o "elo mais fraco", é importante, contudo, reconhecer o papel das pessoas nestas matérias. Por isso, o *Relatório Cibersegurança em Portugal – tema Sociedade* tem vindo a ser publicado anualmente com o objetivo de analisar as atitudes, os comportamentos, a sensibilização e a educação em cibersegurança no país. Esta publicação do Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS), na sua quinta edição, segue a abordagem das anteriores: por um lado, sistematiza e analisa estatísticas disponíveis; por outro, recolhe e produz dados considerados em falta. A maioria dos indicadores refere-se a 2022, mas alguns já contemplam 2023. Sempre que necessário, este documento estabelece articulações com as restantes dimensões da cibersegurança e com outras publicações do Observatório de Cibersegurança do CNCS.

Em termos temáticos, o relatório divide-se em quatro capítulos principais:

a. "Ambiente sociotécnico", onde se apresentam estatísticas sobre o número de utilizadores das tecnologias digitais e a sua exposição ao risco no ciberespaço;
b. "Interesse pela 'cibersegurança' nos *media* e nas pesquisas *online*", através do qual se acompanham indicadores de interesse pelo tema nos *media* e nas pesquisas *online*;
c. "Atitudes e comportamentos", em que são sistematizadas as estatísticas disponíveis sobre as práticas de cibersegurança nas organizações privadas e públicas;
d. "Sensibilização e educação", a parte dedicada à análise dos dados recolhidos sobre as ações de sensibilização e o ensino de cibersegurança e segurança de informação.

Apresentam-se de seguida as principais conclusões deste estudo através de uma análise global e de um conjunto de destaques com os dados mais relevantes.

ANÁLISE GLOBAL[1]

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

TENDÊNCIAS

AMBIENTE SOCIOTÉCNICO, ARTIGOS NOS *MEDIA* E PESQUISAS *ONLINE*

A exposição dos indivíduos e das organizações ao ciberespaço aumentou em 2022 em Portugal e encontra-se acima da média da União Europeia (UE) relativamente a alguns serviços digitais críticos. Houve mais indivíduos a usar a Internet e grande parte das organizações públicas e privadas possuíam ligações de banda larga. Destaca-se um número de indivíduos significativamente acima da média da UE a usar telefonemas e videochamadas pela Internet, mensagens instantâneas e redes sociais.

> “EM 2022, VERIFICOU-SE UM ACENTUADO INCREMENTO DA NOTORIEDADE DA CIBERSEGURANÇA COMO TEMA.”

Em 2022, verificou-se ainda um acentuado incremento da notoriedade da cibersegurança como tema. O número de artigos nos *media* que mencionaram esta palavra e de pesquisas *online* sobre a mesma aumentou de forma assinalável face ao ano anterior. Este incremento estará correlacionado com o nível de impacto de alguns incidentes de cibersegurança registados em Portugal durante esse período, com particular incidência no mês de fevereiro.

ATITUDES E COMPORTAMENTOS

Houve mais empresas em Portugal em 2022 com Políticas de Segurança das Tecnologias da Informação e Comunicação (TIC) definidas do que a média da UE, mas menos de metade tinha documentação deste tipo. Na Administração Pública, quase dois terços dos organismos definiram uma estratégia neste domínio, mas menos do que em anos anteriores. Portanto, embora o país compare bem com o exterior, há trabalho a realizar no âmbito do enquadramento estratégico para a cibersegurança nas organizações em Portugal.

No que diz respeito a medidas concretas, ainda que grande parte das empresas tenha afirmado usar palavras-passe seguras, menos de um terço aplicou o múltiplo fator de autenticação. Na Administração Pública, menos de metade dos organismos tinham esta medida im-

1. Os dados apresentados em “Análise Global” são descritos com valores e respetivas referências em “Destaques” e ao longo de todo o documento.

plementada. Todavia, outras medidas foram aplicadas de forma muito generalizada na Administração Pública, como é o caso da atualização regular do *software*.

As atividades relacionadas com a segurança das TIC foram predominantemente realizadas por fornecedores externos, quando falamos das empresas, e por pessoal interno, no âmbito da Administração Pública. Contudo, tal como em anos anteriores, a Administração Pública viu crescer a sua necessidade de competências em segurança das TIC para os níveis mais elevados dos últimos anos.

Já quanto a recomendações sobre segurança nas TIC disponibilizadas a empregados, verificou-se algum equilíbrio entre os setores público e privado, em que quase metade dos organismos públicos e um pouco mais de metade das empresas afirmaram ter este tipo de recomendação (valor significativamente acima da média da UE no que se refere a empresas)[2].

SENSIBILIZAÇÃO E EDUCAÇÃO

Em 2022, as ações de sensibilização em cibersegurança dirigidas ao público em geral em Portugal, realizadas por organizações que assumem essa missão, ocorreram predominantemente na forma de sessões presenciais e *online* e de cursos *online*. Todavia, tal como verificado em parte no relatório do ano passado, as ações através das redes sociais, da comunicação social e de mobiliário urbano para informação (MUPI), embora em menor número, tiveram um alcance mais elevado. Este alcance exige um menor envolvimento das pessoas comparando com as sessões e os cursos *online*.

Verificou-se também um crescimento das ações dirigidas a crianças e jovens. O tema mais frequente foi o da ciber-higiene em termos genéricos, embora outros temas também tenham tido uma presença importante, como a proteção de dados. Portanto, constata-se a existência de alguma variedade de canais e temas, bem como uma maior granularidade no público escolhido. Ainda persiste a prática de não se realizarem avaliações de impacto destas ações por parte de algumas organizações, embora as que têm mais alcance o façam.

Destacaram-se algumas tendências positivas no que diz respeito à realização de ações de sensibilização nas organizações dirigidas aos empregados no ano de 2022: o número de empresas a sensibilizar os seus empregados para a segurança das TIC aumentou, ocorrendo em quase dois terços das mesmas, e verificou-se um crescimento significativo no número de organismos públicos que verteram em disposições contratuais obrigações neste domínio, fixando-se em cerca de um terço da Administração Pública.

Quanto ao ensino superior especializado em cibersegurança e segurança de informação, o número de cursos continuou a aumentar, com mais duas licenciaturas e um mestrado, e o número de alunos inscritos e diplomados também. Contudo, a percentagem de mulheres inscritas e diplomadas foi relativamente baixo.

2. Embora se realize uma comparação direta entre empresas e Administração Pública neste texto, os dados sobre as primeiras são produzidos com base numa amostra recolhida pelo Eurostat e os segundos com base na totalidade do universo acedido pela DGEEC.

CENÁRIOS DE AMEAÇAS E O FATOR HUMANO

Os resultados principais da análise apresentada devem ser lidos à luz das ameaças que afetam o ciberespaço, pois é em relação a estas que se identificam as vulnerabilidades e as ações de mitigação (que na gestão de risco se designam de "controlos").

O contexto descrito no último relatório do Observatório de Cibersegurança do CNCS sobre Riscos e Conflito (CNCS, 2023) mostra a preponderância de algumas ameaças, como o *ransomware*, o *phishing*, a burla *online*, o comprometimento de contas, diversos tipos de engenharia social e a cibersabotagem. Em relação a estas ameaças, existem formas de proteção que passam pelo comportamento dos indivíduos e das organizações, bem como por processos e estratégias nacionais mais alargados. Algumas ameaças implicam soluções sobretudo técnicas, outras exigem um forte envolvimento do fator humano (ver quadro 1).

Um maior uso das tecnologias digitais aumenta a exposição dos indivíduos aos riscos do ciberespaço e à hipótese de se depararem com um *email* de *phishing* ou uma tentativa de burla *online*. A visível notoriedade do tema nos *media* e nas pesquisas *online*, todavia, pode significar que as pessoas estão mais atentas e eventualmente mais informadas sobre os cuidados que devem aplicar. Por sua vez, de um modo transversal, a ausência de Políticas e Estratégias de Segurança de Informação em algumas organizações pode significar que não existem automatismos suficientes de prevenção e resposta a incidentes. No entanto, a atualização de *software* regular e o uso de palavras-passe seguras ajudam a reduzir grande parte dos riscos *online*. A parca implementação do múltiplo fator de autenticação, pelo contrário, coloca demasiado peso na palavra-passe como elemento de proteção dos sistemas, facilitando o comprometimento de contas e outros tipos de incidentes subsequentes.

A falta de recursos humanos especializados na Administração Pública tem consequências negativas na capacidade de proteção contra quase todas as ameaças, com particular relevância em relação às que compreendem uma maior sofisticação técnica, como o *ransomware* e a cibersabotagem. A falta de especialistas em geral diminui o conhecimento dentro das organizações, o qual pode ser crítico para a adoção de tecnologias e boas práticas de cibersegurança. Associado à questão do conhecimento disponível encontra-se o problema da insuficiente disponibilização de recomendações sobre boas práticas aos empregados das organizações, algo que afeta em particular as medidas de mitigação do âmbito da ciber-higiene, fundamentais para o combate ao *phishing* e a outras formas de engenharia social.

Por fim, a existência de ações de sensibilização massificadas - e algumas delas com precisão nos públicos-alvo e nos temas -, o incremento do número de organizações que realizam ações de sensibilização dirigidas aos seus empregados, bem como o aumento do número de cursos especializados, de inscritos e de diplomados em cibersegurança e segurança de informação, têm um efeito mais positivo e transversal na resposta às ameaças. A disseminação de boas práticas de ciber-higiene junto de todos os cidadãos e dos trabalhadores em particular e a promoção de conhecimento especializado em possíveis profissionais contribuem para que o saber que ainda falta nas organizações seja desenvolvido.

Quadro 1

RELAÇÃO ENTRE RESULTADOS DESTE RELATÓRIO E PRINCIPAIS AMEAÇAS AO CIBERESPAÇO DE INTERESSE NACIONAL, EM 2022/2023

Resultados de *Sociedade 2023* / Ameaças em *Riscos e Conflitos 2023* (CNCS, 2023)	Ransomware	Phishing Smishing Vishing	Burla *online*	Compro-metimento de contas / tentativa de *login*	Engenharia social (várias)	Cibersabotagem / indisponibilidade
Maior risco fruto de aumento dos usos da Internet e serviços digitais						
Maior notoriedade do tema da cibersegurança						
Insuficiente adoção de Políticas e Estratégias de Segurança de Informação (embora tendência positiva nas empresas)						
Aplicação elevada de algumas medidas nas organizações (e.g. atualização do *software*, uso de palavras-passe seguras)						
Aplicação insuficiente de algumas medidas nas organizações (e.g. múltiplo fator de autenticação)						
Elevada necessidade de competências em segurança das TIC na Administração Pública						
Insuficiente disponibilização de recomendações sobre segurança das TIC nas organizações (embora tendência positiva nas empresas)						
Existência de ações de sensibilização dirigidas ao público em geral com canais variados e maior precisão nos públicos e temas						
Mais organizações a sensibilizar os seus empregados						
Mais cursos do ensino superior especializados, bem como alunos inscritos e diplomados						

 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

Além de caracterizar a componente social da cibersegurança em Portugal, este relatório procura acompanhar os indicadores que se correlacionam com a atual Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENSC). Esta correlação centra-se em particular num dos seis eixos de intervenção da ENSC, o Eixo 2 - Prevenção, educação e sensibilização. Destacam-se quatro conclusões correlacionadas com este eixo:

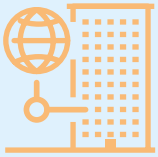
1. Verificam-se tendências positivas nas práticas de sensibilização em cibersegurança, tais como a elevada variedade de canais usados, a especificidade de públicos, bem como uma aplicação mais consistente nas organizações. Persiste uma tendência negativa na falta de avaliação de impacto em muitas das entidades que realizam estas ações de sensibilização.
2. Há uma tendência positiva no crescimento de ações de sensibilização dirigidas a crianças e jovens. Contudo, mantém-se uma tendência negativa na falta de mulheres inscritas e diplomadas em cursos superiores especializados nesta área, comparando com a área das TIC em geral.
3. A maior presença da cibersegurança na educação formal, nomeadamente no ensino superior, é uma tendência positiva;
4. Também é uma tendência positiva o aumento do número de alunos inscritos e diplomados em cursos especializados em cibersegurança, embora ainda de forma insuficiente face ao total de alunos diplomados em cursos de TIC.

DESTAQUES

AMBIENTE SOCIOTÉCNICO, ARTIGOS NOS *MEDIA* E PESQUISAS *ONLINE* SOBRE "CIBERSEGURANÇA" EM PORTUGAL

A percentagem de indivíduos a usar a Internet aumentou, passando de 82% dos indivíduos em 2021 para 85% em 2022 (Eurostat).

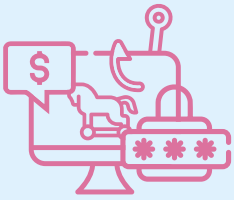
Quase todas as organizações privadas e públicas em Portugal possuem ligações de banda larga à Internet em 2022 (e.g. 100% das Câmaras Municipais) (Eurostat e DGEEC).



Certos serviços digitais críticos para a cibersegurança, em 2022, foram usados por mais indivíduos em Portugal do que a média da UE: o *email* (88% em Portugal, +2 pp do que a média da UE); os telefonemas e videochamadas pela Internet (81%, +8 pp); mensagens instantâneas (92%, +12 pp); as redes sociais (79%, +14 pp) e o banco *online* (68%, +2 pp) (Eurostat).

Em 2022, houve mais artigos publicados nos *media* a usar o termo "cibersegurança" e mais pesquisas *online* com esta palavra do que em 2021, com particular incidência no mês de fevereiro, período respeitante ao registo de incidentes de elevado impacto em Portugal (Mediacloud e Google Trends).

Associadas à pesquisa no motor de busca Google pela palavra "cibersegurança" em 2022 ocorreram pesquisas ligadas à componente educacional e institucional da cibersegurança. Aos termos como "*phishing*" e "*ransomware*" foram associadas pesquisas sobre os meios através dos quais estas ameaças se concretizam e a classe de incidentes a que pertencem (Google Trends).



ATITUDES E COMPORTAMENTOS EM PORTUGAL

Em 2022, houve mais empresas em Portugal com uma Política de Segurança das TIC definida e revista nos últimos 24 meses (43%) do que a média da UE (32%) (Eurostat).

A autenticação através de palavra-passe segura foi a medida de segurança das TIC mais aplicada pelas empresas em 2022 (84%), mas apenas cerca de um terço (28%) aplicou o múltiplo fator de autenticação (Eurostat).

Em 2022, verificou-se uma forte presença de fornecedores externos nas atividades relacionadas com a segurança das TIC nas empresas (72%) (Eurostat).

Mais de metade das empresas (54%), em 2022, afirmou ter recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC, valor bastante acima da média da UE (37%) (Eurostat).

Menos de metade das empresas disponibilizou guiões de segurança das TIC para o acesso remoto (49%) ou para reuniões *online* à distância (32%) em 2022 (Eurostat).

Na Administração Pública, 59% dos organismos afirmou ter uma Estratégia para a Segurança de Informação definida em 2022, o mesmo valor do ano anterior (DGEEC).

A medida de segurança das TIC mais utilizada na Administração Pública em 2022 foi a atualização regular do *software*. Menos de metade aplicou o múltiplo fator de autenticação (DGEEC).

A necessidade de competências em segurança das TIC continuou elevada no conjunto da Administração Pública, passando-se de 69% dos organismos em 2021 para 74% em 2022 (DGEEC).

Em 2022, quanto mais as Câmaras Municipais referem ter estratégias para a segurança de informação definidas menos manifestam necessidade elevada de reforço das competências em segurança das TIC (DGEEC).

Ao contrário das empresas, na Administração Pública, em 2022, predominou o pessoal do próprio organismo a realizar atividades relacionadas com a segurança das TIC (DGEEC).

Menos de metade dos organismos do conjunto da Administração Pública (46%) indicou, em 2022, ter recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC, menos 1 pp do que no ano anterior (DGEEC).

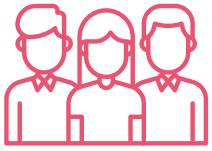
Em 2022, apenas 3% dos organismos do conjunto da Administração Pública tinha seguro contra incidentes de segurança nas TIC (DGEEC).

EDUCAÇÃO E SENSIBILIZAÇÃO EM PORTUGAL

As ações de sensibilização em cibersegurança mais frequentes, dirigidas ao público em geral por organizações que assumem essa missão, em 2022, foram as sessões presenciais e *online* e os cursos *online* (Inquérito CNCS).

Embora impliquem menos envolvimento do público e se realizem em menor número do que as sessões e os cursos *online*, as ações de sensibilização dirigidas a públicos externos realizadas através das redes sociais, da comunicação social e de MUPI tiveram, em 2022, um alcance mais elevado (Inquérito CNCS).

Verificou-se, em 2022/2023, um aumento das ações de sensibilização em cibersegurança dirigidas a públicos externos orientadas a crianças e jovens (Inquérito CNCS).



O tema mais frequente tratado nas ações de sensibilização dirigidas a um público externo, em 2022/2023, foram as boas práticas genéricas de ciber-higiene, a proteção de dados, privacidade e direitos e o *cyberbullying* (Inquérito CNCS).

A maioria das entidades que realizaram ações de sensibilização em cibersegurança dirigidas a públicos externos não avaliaram, em 2022/2023, o impacto das mesmas nesses públicos (Inquérito CNCS).

A percentagem de empresas a realizar ações de sensibilização para os seus empregados em matéria de segurança das TIC aumentou 9 pp em 2022, fixando-se em 63% (Eurostat).

A percentagem de organismos da Administração Pública a converterem para disposições contratuais as obrigações em matéria de segurança das TIC dirigidas ao seu pessoal ao serviço aumentou 7 pp, passando de 21% em 2021 para 28% em 2022 (DGEEC).

O número de cursos de ensino superior especializados em cibersegurança e segurança de informação registados aumentou de 25 em 2022 para 28 em 2023. Foram criadas mais duas licenciaturas e um mestrado (DGES – recolha CNCS).

Em 2023, existem 13 cursos TESP, 11 mestrados, três licenciaturas e um doutoramento especializados em cibersegurança e segurança de informação (DGEEC – recolha CNCS).

A maioria dos cursos superiores especializados em cibersegurança e segurança de informação concentra-se no Norte e na Área Metropolitana de Lisboa e é realizado por Instituições do ensino público (DGEEC – recolha CNCS).

O número de alunos inscritos em cursos do ensino superior especializados em cibersegurança e segurança da informação aumentou 24% em 2022/2023. O número de diplomados também aumentou, em 34%, no ano letivo 2021/2022 (DGEEC – recolha CNCS) – correspondem a 2,5% do número de diplomados em cursos de TIC em 2022 (Pordata).

A percentagem de mulheres inscritas nestes cursos foi de 10% em 2022/2023 e de diplomadas foi de 7% em 2021/2022 (DGEEC – recolha CNCS) – nos cursos de TIC o valor de diplomadas é de 20,5% (Pordata).

“O PRESENTE RELATÓRIO CARACTERIZA O ESTADO DA COMPONENTE SOCIAL DA CIBERSEGURANÇA NO PAÍS, DE MODO A IDENTIFICAR TENDÊNCIAS E ASPETOS A MELHORAR, PROCURANDO INFORMAR AS ESTRATÉGIAS DE CAPACITAÇÃO HUMANA A ESTE NÍVEL.”

B. INTRODUÇÃO

As organizações têm um papel central na cibersegurança de um país, não só porque são responsáveis pelo funcionamento de serviços essenciais e críticos para a sociedade, como também porque têm uma influência direta sobre os seus empregados na adoção de boas práticas de cibersegurança, tendo estas potencial para se repercutir na sociedade em geral. Esta quinta edição do *Relatório Cibersegurança em Portugal – tema Sociedade* tem particular atenção às organizações e à dimensão social das práticas de cibersegurança nesse contexto, nomeadamente nas empresas e na Administração Pública.

Tal como nas edições anteriores, este estudo recolhe e sistematiza informação disponível, e produz a que se encontrar em falta, sobre atitudes, comportamentos, educação e sensibilização relativamente à cibersegurança em Portugal. Assim, o presente relatório caracteriza o estado da componente social da cibersegurança no país, de modo a identificar tendências e aspetos a melhorar, procurando informar as estratégias de capacitação humana a este nível.

O documento é estruturado em quatro capítulos principais: "ambiente sociotécnico", no qual se acompanham os dados sobre a quantidade de utilizadores de serviços digitais e o seu nível de exposição ao risco; "interesse pela 'cibersegurança' nos *media* e nas pesquisas *online*", em que se realiza uma análise à quantidade de artigos publicados nos *media* e de pesquisas realizadas com o uso da palavra "cibersegurança", percebendo-se assim os níveis de notoriedade deste tema; "atitudes e comportamentos", onde são sistematizadas as últimas estatísticas sobre as práticas de cibersegurança nas empresas e na Administração Pública; e "sensibilização e educação", em que se recolhem e analisam dados relativos aos cursos e alunos do ensino superior de cibersegurança e segurança de informação. No final do documento, entre outros aspetos, é possível aceder a um *briefing* sobre a ENSC dedicado aos indicadores que permitem estabelecer uma correlação com certas linhas de ação da atual ENSC, algumas notas metodológicas, bem como uma explicação sobre termos, siglas e abreviaturas usados ao longo do texto.

“A PERCENTAGEM DE INDIVÍDUOS A USAR A INTERNET EM PORTUGAL CONTINUA A AUMENTAR.”

C. AMBIENTE SOCIOTÉCNICO

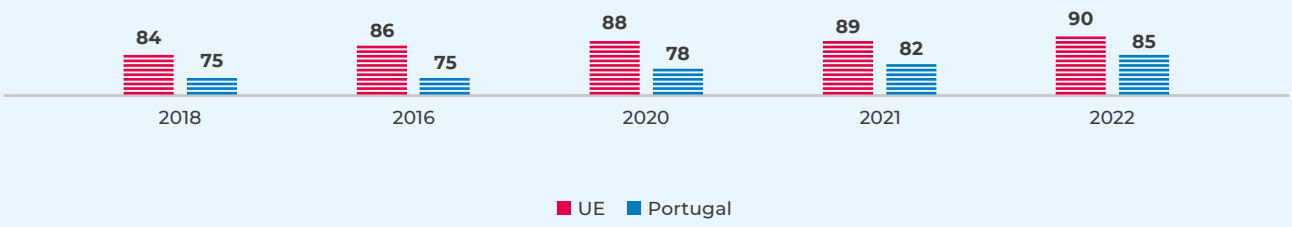
Por "ambiente sociotécnico" entende-se os indicadores de uso das tecnologias digitais que expressam o grau de exposição dos utilizadores ao ciberespaço. Um maior ou menor uso do ciberespaço implica uma maior ou menor exposição às ameaças que o afetam.

O USO DA INTERNET

Considerando dados do Eurostat, a percentagem de indivíduos a usar a Internet em Portugal continua a aumentar. Em 2022, verificou-se um aumento de 3 pp face a 2021, passando-se de 82% para 85%[3] de indivíduos a terem usado a Internet nos últimos 3 meses. Esta tendência verifica-se pelo menos desde 2019. Não obstante, este valor continua abaixo da média da UE, que registou 90% em 2022. Uma distância que diminuiu em relação a anos anteriores, nos quais a diferença foi, em geral, maior do que 5 pp.

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.

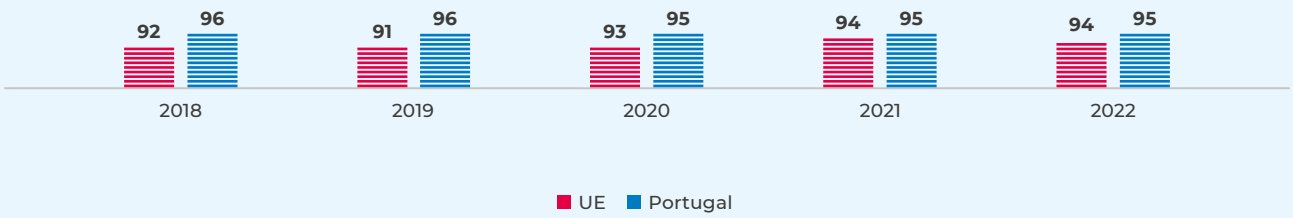
Fonte: Eurostat, 2023a

3. Os valores são arredondados ao longo de todo o documento.

No âmbito das organizações, verificou-se uma estabilização em 95% de empresas[4] em Portugal que usaram DSL ou outra conexão de banda larga, entre 2020 e 2022, sendo que o país, nesta matéria, se encontra ligeiramente acima da média da UE, em 1 pp.

Figura 2

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



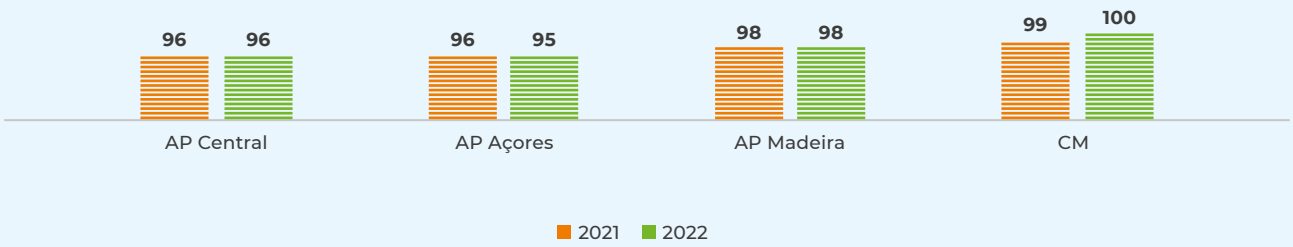
*Até 2019 os dados são referentes à UE a 28, a partir de 2020 passou a considerar-se os dados referentes à UE a 27.

Fonte: Eurostat, 2023b

No âmbito dos organismos da Administração Pública, de acordo com dados da Direção-Geral de Estatísticas da Educação e Ciência (DGEEC), o uso de ligação fixa de banda larga à Internet em 2022 foi generalizado, atingindo os 100% nas Câmaras Municipais e os 96% na Administração Pública Central.

Figura 3

ENTIDADES DA ADMINISTRAÇÃO PÚBLICA COM LIGAÇÃO FIXA DE BANDA LARGA À INTERNET, EM PORTUGAL. *ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS* (%)



Fonte: DGEEC, 2023a e 2023b

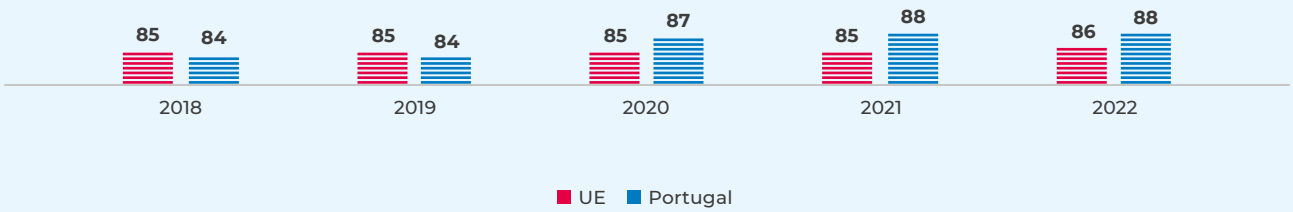
4. Empresas com mais do que 10 empregados, sem contar com o setor financeiro.

OS USOS DE SERVIÇOS CRÍTICOS PARA A CIBERSEGURANÇA

Quanto a alguns serviços digitais particularmente expostos a ciberataques, constata-se que em Portugal a percentagem de indivíduos a usar o *email* nos últimos três meses estabilizou nos 88% em 2022, tal como no ano anterior, mantendo-se acima da média da UE em 2 pp.

Figura 4

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



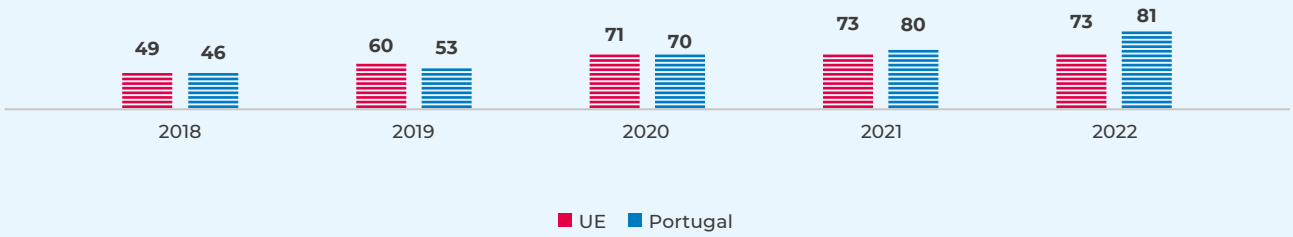
*Até 2019 os dados são referentes à UE a 28, a partir de 2020 passou a considerar-se os dados referentes à UE a 27.

Fonte: Eurostat, 2023c

Desde pelo menos 2018 que o uso do telefone e videochamadas via Internet pelos indivíduos tem aumentado em Portugal, verificando-se um crescimento muito acentuado em 2020 (+17 pp) e 2021 (+10 pp), coincidindo com o período da pandemia da Covid-19 e a maior adoção de processos de trabalho à distância. Em 2022, o valor fixou-se em 81%, mais 1 pp do que em 2021. Desde 2021 que Portugal tem valores acima da UE a este respeito, registando em 2022 mais 8 pp do que a média da UE.

Figura 5

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



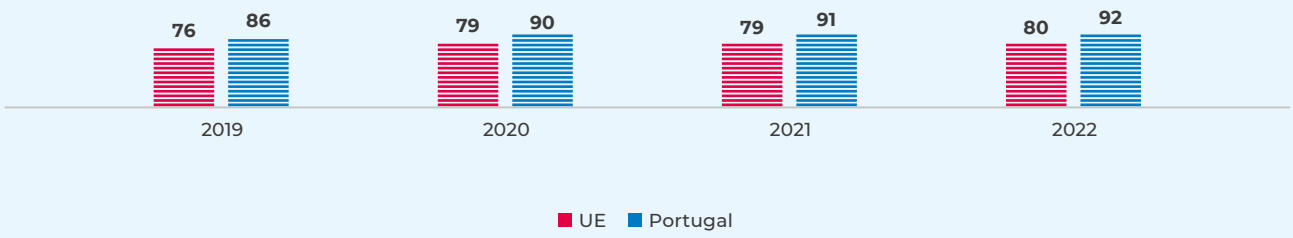
*Até 2019 os dados são referentes à UE a 28, a partir de 2020 passou a considerar-se os dados referentes à UE a 27.

Fonte: Eurostat, 2023c

O uso de mensagens instantâneas aumentou ligeiramente em Portugal entre 2021 e 2022, de 91% para 92% dos indivíduos. Um valor significativamente acima da média da UE, que se fixou em 80%.

Figura 6

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



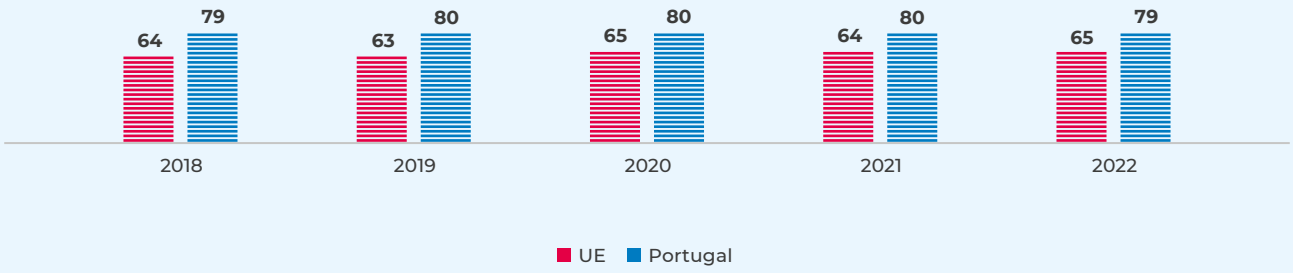
*Até 2019 os dados são referentes à UE a 28, a partir de 2020 passou a considerar-se os dados referentes à UE a 27.

Fonte: Eurostat, 2023c

Continua a existir uma percentagem de indivíduos relativamente elevada a usar redes sociais em Portugal, um valor que se fixa em 79% em 2022, contra 65% na média da UE.

Figura 7

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



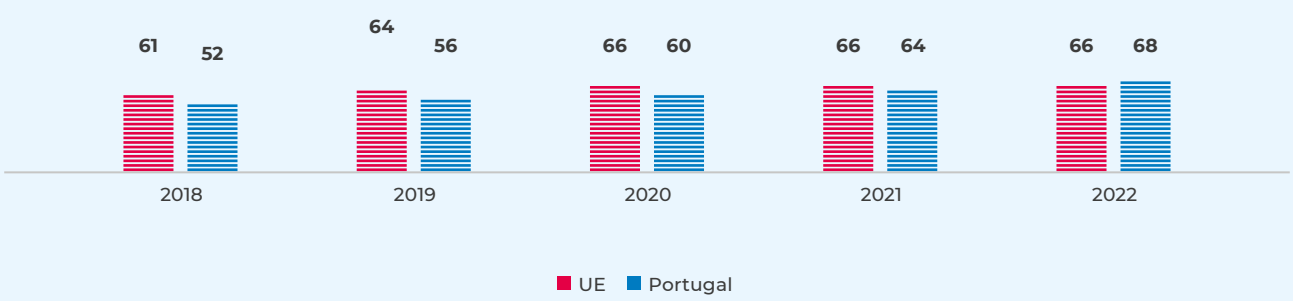
*Até 2019 os dados são referentes à UE a 28, a partir de 2020 passou a considerar-se os dados referentes à UE a 27.

Fonte: Eurostat, 2023c

Pela primeira vez há mais indivíduos a usarem o banco *online* em Portugal do que a média da UE, atingindo-se os 68% em 2022, mais 4 pp do que em 2021 e mais 2 pp do que a média da UE.

Figura 8

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



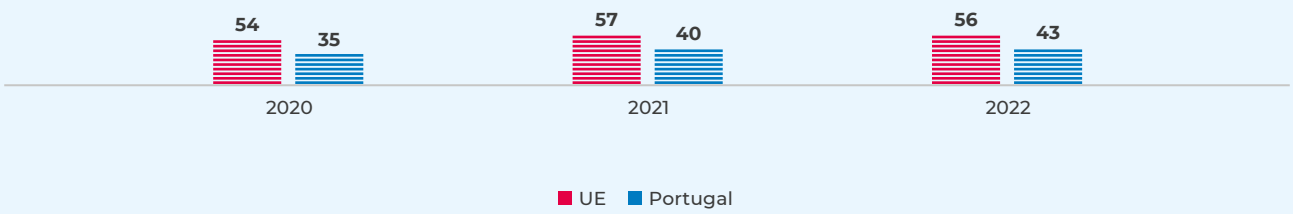
*Até 2019 os dados são referentes à UE a 28, a partir de 2020 passou a considerar-se os dados referentes à UE a 27.

Fonte: Eurostat, 2023c

No que diz respeito às compras *online* em Portugal, há mais indivíduos a realizá-las em 2022 do que em 2021, atingindo-se o valor de 43%, mais 3 pp do que no ano anterior. Não obstante, este número está abaixo da média da UE em 13 pp.

Figura 9

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



Fonte: Eurostat, 2023d

DESTAQUES

- A percentagem de indivíduos a usar a Internet continua a aumentar em Portugal, passando-se de 82% em 2021 para 85% em 2022. Contudo, este valor está abaixo da média da UE, que se fixou em 90%.
- Quase a totalidade das organizações privadas e públicas em Portugal usou ligações de banda larga à Internet, nomeadamente 95% das empresas com mais de dez empregados, 96% da Administração Pública Central e 100% das Câmaras Municipais.
- Verifica-se que em Portugal certos serviços digitais críticos para a cibersegurança foram usados por mais indivíduos do que a média da UE: o *email* (88% em Portugal, +2 pp do que a média da UE); os telefonemas e videochamadas pela Internet (81%, +8 pp); as mensagens instantâneas (92%, +12 pp); as redes sociais (79%, +14 pp) e o banco *online* (68%, +2 pp).

ESTADO DO AMBIENTE SOCIOTÉCNICO

Internet em 2022 – mais utilizadores.

Aspetos críticos em 2022 – uso acima da média da UE, em termos de número de indivíduos, de determinados serviços críticos para a cibersegurança, como o *email* (alvo de campanhas de *phishing*), telefonemas e videochamadas pela Internet (meio para ataques de engenharia social e recolha de informação sensível), mensagens instantâneas (objeto de campanhas de *smishing* e outras formas de engenharia social), redes sociais (plataformas onde ocorrem furtos de identidade, comprometimentos de contas, recolhas de informação sensível e campanhas de desinformação) e banco *online* (alvo de comprometimento de contas e fraudes bancárias).

“O MAIOR INTERESSE PELA 'CIBERSEGURANÇA' EM 2022 PRESENTE NOS *MEDIA* TAMBÉM SE CONFIRMA NAS PESQUISAS NO MOTOR DE BUSCA GOOGLE.”

D. INTERESSE PELA "CIBERSEGURANÇA" NOS MEDIA E NAS PESQUISAS *ONLINE*

O interesse pela "cibersegurança" como tema pode ser acompanhado através da análise da sua presença nos *media* e nas pesquisas *online*. A saliência de assuntos ligados a esta área em notícias e nas pesquisas em motores de busca é sintoma da sua importância na agenda mediática e digital. Estes dados permitem conjeturar possíveis correlações com alguns incidentes com impacto, períodos de maior número de incidentes ou a emergência de ameaças.

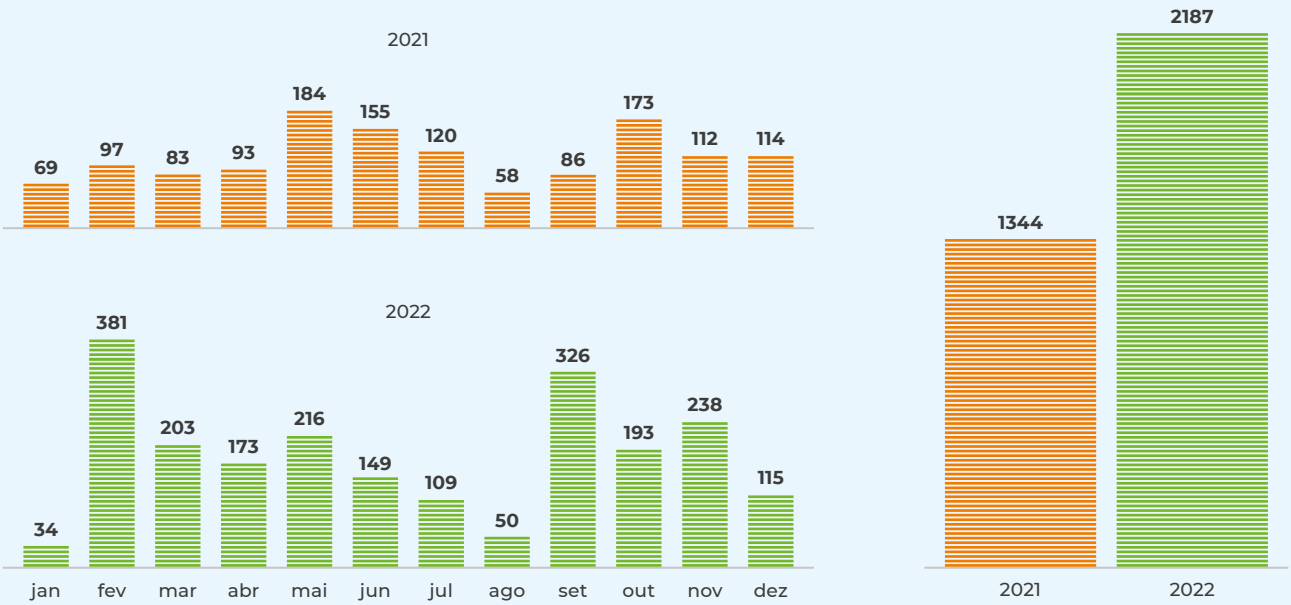
ARTIGOS NOS *MEDIA* QUE MENCIONAM A PALAVRA "CIBERSEGURANÇA"

Através da plataforma *mediacloud*[5], é possível verificar o número de artigos publicados nos media que mencionaram o termo "cibersegurança" em Portugal. Comparando 2022 com 2021, verificou-se um crescimento de 67% no número de artigos, os quais passaram de 1344 em 2021 para 2187 em 2022. Na comparação mensal, é notável o elevado número de artigos publicados em fevereiro de 2022 (381) face ao período homólogo (97), o que representa um aumento de 293%, algo eventualmente associado aos incidentes com muito impacto que ocorreram no país nesse trimestre. O significativo número de artigos com este termo registados em setembro de 2022 (326) coincide com o momento que se seguiu ao ataque de *ransomware* que atingiu a TAP. Estes dados demonstram a forte presença da cibersegurança nos *media* em 2022, um ano marcado por incidentes com grande visibilidade social (ver CNCS, 2023).

5. Para mais detalhe, consultar as seguintes páginas: https://www.mediacloud.org/ e www.mediacloud.org/documentation/search-tool-guide. Para a recolha destes dados, foram utilizados 90 meios de comunicação, que podem ser consultados aqui: https://search.mediacloud.org/collections/34412337 [consultado a 07/11/2023]

Figura 10

NÚMERO DE ARTIGOS PUBLICADOS NOS *MEDIA* QUE MENCIONARAM O TERMO "CIBERSEGURANÇA" EM PORTUGAL



Fonte: Mediacloud

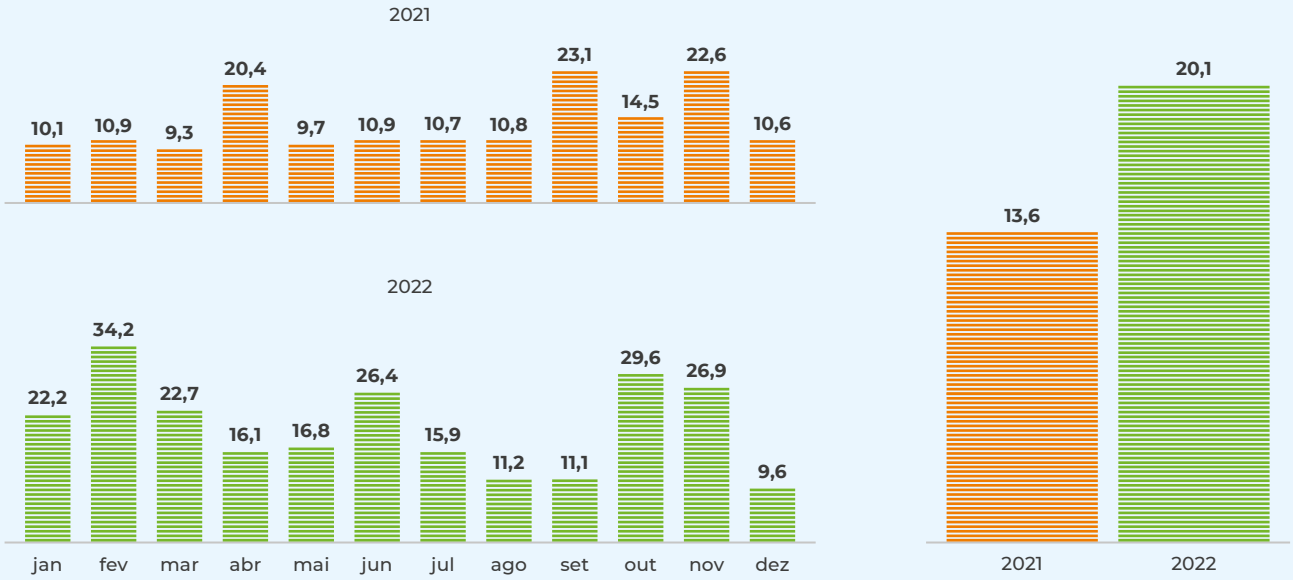
PESQUISAS PELA PALAVRA "CIBERSEGURANÇA"

O maior interesse pela "cibersegurança" em 2022 presente nos *media* também se confirma nas pesquisas no motor de busca Google analisadas através da plataforma Google Trends[6], realidade já constatada no relatório do ano passado no que se refere ao primeiro semestre. À luz do índice de popularidade relativa com base nas pesquisas realizadas[7], verificou-se uma maior popularidade em 2022 (média de 20,1) do que em 2021 (média de 13,6). A maior popularidade no mês fevereiro de 2022 (34,2) em comparação com o período homólogo (10,9) coincide com a elevada presença do termo "cibersegurança" em artigos nos *media* referida anteriormente e com os incidentes de elevado impacto registados nesse período.

6. Para mais detalhe consultar a seguinte página: https://trends.google.pt/trends/ [consultado a 07/11/2023]
7. "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)"

Figura 11

ÍNDICE DE PESQUISAS GOOGLE COM O TERMO “CIBERSEGURANÇA” (MÉDIA) EM PORTUGAL*



*Popularidade relativa: média dos valores semanais, entre 0 e 100, em que 0 significa popularidade relativa do termo de busca muito baixa (valor mínimo) e 100 popularidade relativa do termo de busca muito alta (valor máximo).

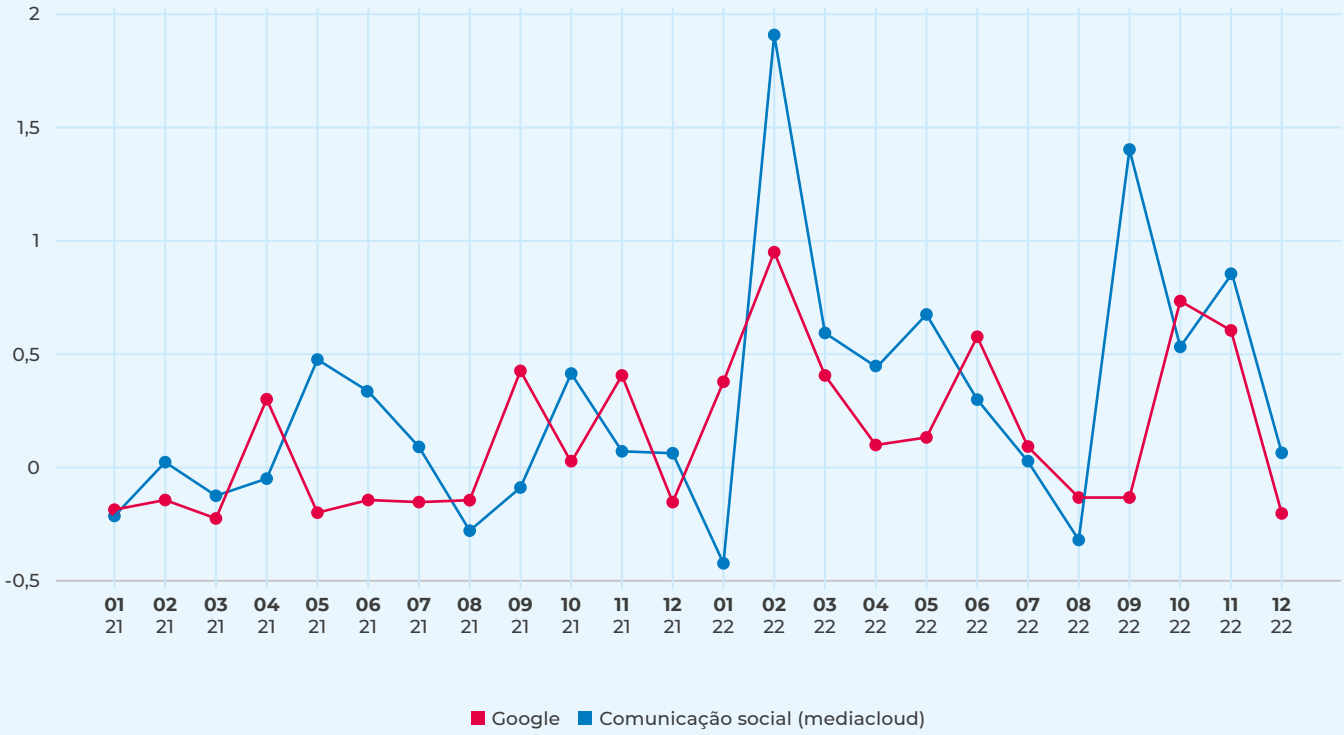
Fonte: Google Trends

Comparando diretamente os dados recolhidos nas plataformas Mediacloud e Google Trends, confrontando a saliência mediática e a popularidade de pesquisas que usam o termo “cibersegurança”, após a normalização dos dados à luz da sua média e desvio padrão (Z-score)[8], constata-se a existência de picos particularmente elevados em 2022 e alguma correlação entre os dois indicadores nesses períodos. Destaca-se, como referido anteriormente, o mês de fevereiro de 2022, em que há um significativo aumento no número de artigos publicados acompanhado de um crescimento relevante no número de pesquisas *online*. O mesmo acontece em setembro, mas com um efeito maior em outubro no que se refere às pesquisas *online*. Como mencionado, a existência de incidentes com muito impacto nestes períodos poderá ter tido consequências numa maior mediatização do assunto e numa maior procura de informação *online*.

8. Se o valor for zero, é igual à média da sua série temporal. Se o valor for dois, está dois desvios padrão acima da média da sua série temporal.

Figura 12

COMPARAÇÃO ENTRE O NÚMERO DE ARTIGOS PUBLICADOS NOS *MEDIA* E ÍNDICE DE PESQUISAS GOOGLE COM O TERMO "CIBERSEGURANÇA" EM PORTUGAL*



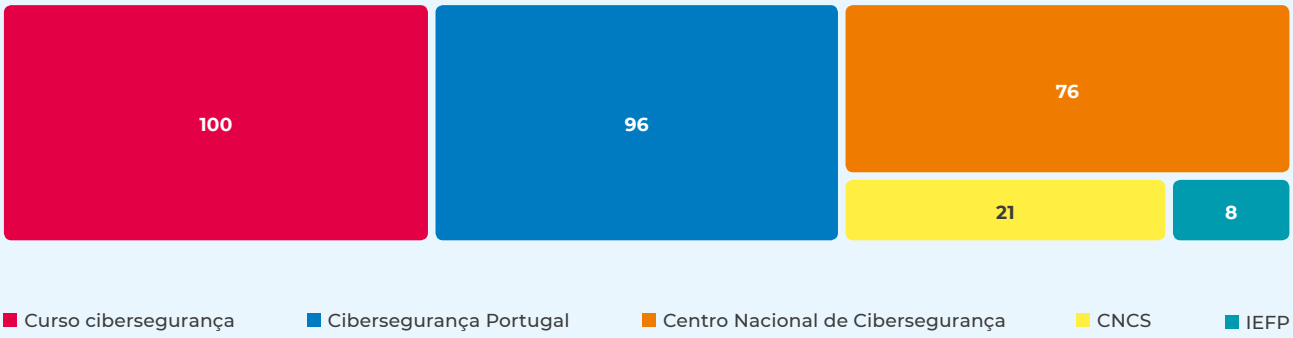
*Comparação realizada com base no desvio padrão.

Fonte: Google Trends e Mediacloud

Retomando os dados recolhidos no Google Trends, os quatro termos mais utilizados em associação à palavra "cibersegurança" nas pesquisas em causa foram "curso", "Portugal", "Centro Nacional de Cibersegurança", "CNCS" e "iefp". Este tipo de termos indicia o predomínio de pesquisas ligadas à educação (já verificada no relatório do ano passado) e à componente nacional e institucional da cibersegurança.

Figura 13

ÍNDICE GOOGLE DE CONSULTAS RELACIONADAS COM AS PESQUISAS PELO TERMO "CIBERSEGURANÇA", EM PORTUGAL, 2022*



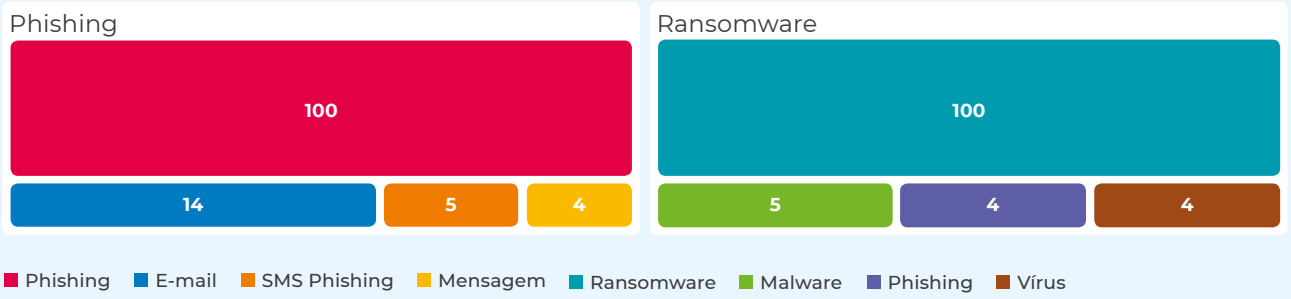
*Popularidade relativa: média dos valores semanais, entre 0 e 100, em que 0 significa popularidade relativa do termo de busca muito baixa (valor mínimo) e 100 popularidade relativa do termo de busca muito alta (valor máximo).

Fonte: Google Trends

Tendo em conta a importância do *phishing*, devido à quantidade de incidentes, e do *ransomware*, pelo seu impacto (CNCS, 2023), considerou-se também as palavras associadas a estas pesquisas, de modo a identificar campos semânticos e com isso preocupações ou necessidades dos utilizadores. Associadas às pesquisas sobre "*phishing*" em 2022, surgem predominantemente os termos "*email*", "*SMS phishing*" e "mensagem", o que remete para o modo através do qual o *phishing* chega aos utilizadores, o *email*, e para outros veículos de envio de mensagens fraudulentas, como o SMS. No caso da palavra "*ransomware*", os termos dominantes associados foram "*malware*", "*phishing*" e "vírus", o que remete para a classe de incidentes a que corresponde esta ameaça, nos casos de "*malware*" e "vírus", e para um dos modos através dos quais esta ameaça pode ser instalada num dispositivo, o "*phishing*", embora eventualmente, em muitos casos, se tratem de *emails* que não recolhem informação mas apenas distribuem *malware*.

Figura 14

ÍNDICE GOOGLE DE CONSULTAS RELACIONADAS COM AS PESQUISAS PELOS TERMOS "*PHISHING*" E "*RANSOMWARE*", EM PORTUGAL, 2022*

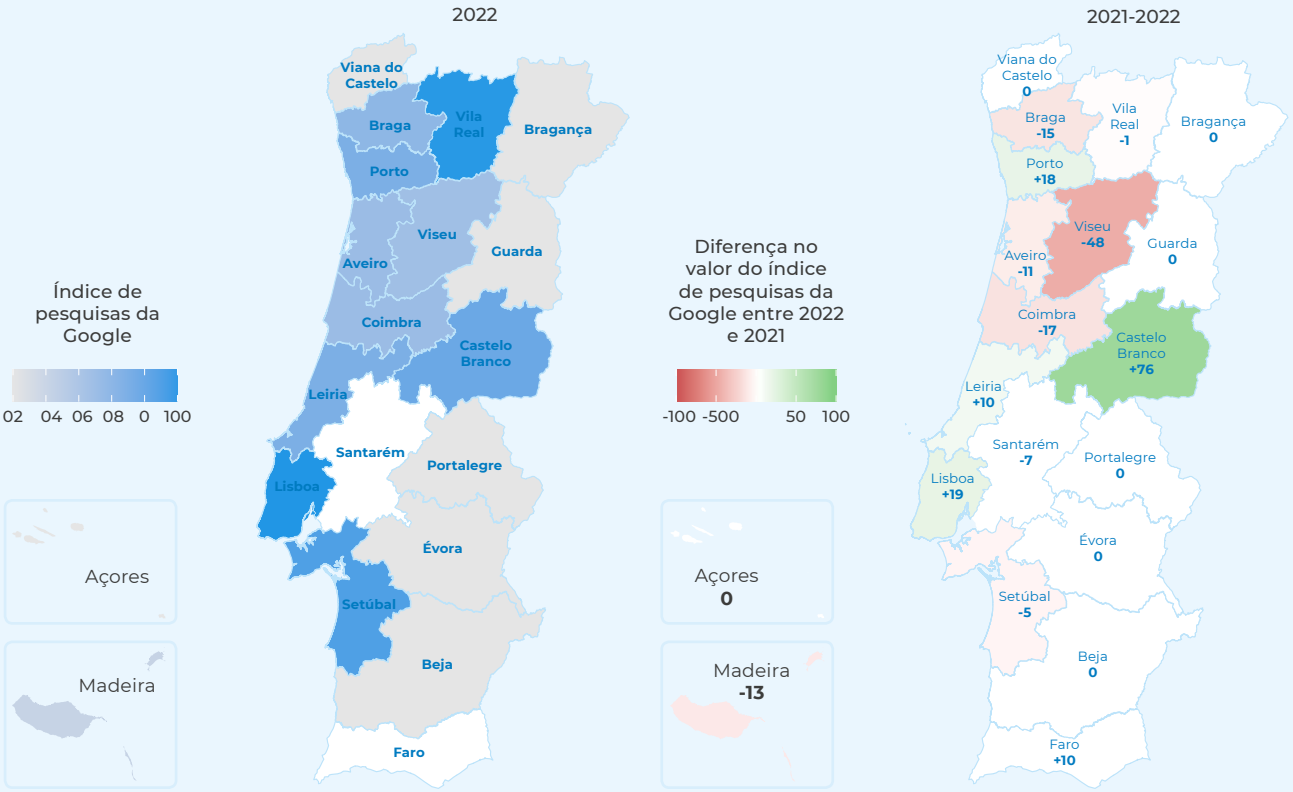


*Popularidade relativa: média dos valores semanais, entre 0 e 100, em que 0 significa popularidade relativa do termo de busca muito baixa (valor mínimo) e 100 popularidade relativa do termo de busca muito alta (valor máximo).

Fonte: Google Trends

Figura 15

ÍNDICE GOOGLE DE PESQUISAS COM O TERMO "CIBERSEGURANÇA" POR REGIÃO, EM PORTUGAL*



*Popularidade relativa: média dos valores semanais, entre 0 e 100, em que 0 significa popularidade relativa do termo de busca muito baixa (valor mínimo) e 100 popularidade relativa do termo de busca muito alta (valor máximo).

Fonte: Google Trends

Do ponto de vista regional, verificou-se um valor mais elevado no índice de pesquisas da Google pela palavra "cibersegurança" nos distritos de Lisboa e Vila Real do que nas restantes regiões em 2022, sendo que há um maior pendor no Norte litoral do que no interior e Sul do país[9]. Comparativamente ao ano anterior, verificou-se um crescimento significativo em Castelo Branco neste índice de pesquisas, em contraciclo com as restantes regiões do interior do país. Viseu, pelo contrário, apresenta uma variação oposta.

DESTAQUES

- Em 2022, verificou-se um aumento assinalável no número de artigos publicados nos *media* em Portugal face a 2021, com particular destaque para os meses de fevereiro e setembro, períodos nos quais ocorreram incidentes de elevado impacto social.
- O índice de pesquisas da Google também revela um aumento significativo da popularidade do termo "cibersegurança" em 2022 em comparação com 2021, com particular relevância, mais uma vez, para o mês de fevereiro, mas também para os meses de outubro e novembro. Durante estes períodos, o número de pesquisas tendeu a acompanhar o número de artigos publicados.
- As pesquisas no Google pela palavra "cibersegurança" foram acompanhadas predominantemente por outros termos que remeteram para os aspetos educacionais e institucionais da cibersegurança. As pesquisas por "*phishing*" e "*ransomware*" foram sobretudo acompanhadas por termos ligados aos meios através dos quais estes ataques se realizam e às classes de incidentes a que pertencem.
- O índice de pesquisas da Google pelo termo "cibersegurança" mostrou uma maior incidência no Norte e litoral do país do que no Sul e interior.

9. Este cálculo é proporcional à dimensão populacional da região e não representa os números absolutos sobre as consultas efetuadas: "um valor maior significa uma proporção maior de consultas, não uma contagem absoluta maior" (Google Trends).

“A NECESSIDADE DE REFORÇO DE COMPETÊNCIAS EM SEGURANÇA DAS TIC CONTINUA MUITO ELEVADA NA ADMINISTRAÇÃO PÚBLICA.”

E. ATITUDES E COMPORTAMENTOS

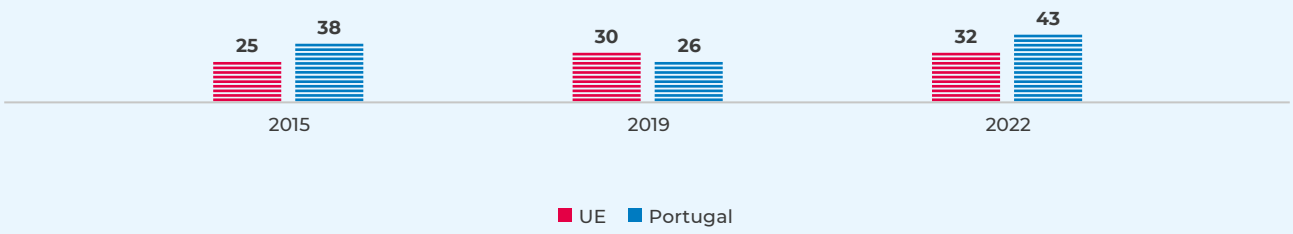
Relativamente às atitudes e comportamentos, a edição deste ano do presente relatório centra-se na análise de dados sobre as empresas e os organismos do setor público, considerando as estatísticas disponibilizadas pelo Eurostat e pela DGEEC.

CIBERSEGURANÇA NAS EMPRESAS

O Inquérito à utilização das TIC nas empresas, realizado pelo Eurostat (2023a-g) e pelo Instituto Nacional de Estatística (INE) para Portugal, apresenta atualizações importantes em 2022 relativamente à componente de segurança. À luz destes dados, verifica-se que em Portugal existiam mais empresas[10] com Política de Segurança das TIC definida e revista pelo menos nos últimos 24 meses em 2022 (43%) do que em 2019[11] (26%) e do que a média da UE (32%).

Figura 16

EMPRESAS COM POLÍTICA DE SEGURANÇA DAS TIC DEFINIDA E REVISTA PELO MENOS NOS ÚLTIMOS 24 MESES (%)



Fonte: Eurostat, 2023e

10. Empresas com mais do que 10 empregados, sem contar com o setor financeiro.
11. Último ano da série antes de 2022.

Quanto a medidas de segurança das TIC utilizadas nas empresas, constata-se que grande parte das medidas foi menos aplicada em Portugal em 2022 do que em 2019, como, por exemplo, a avaliação de riscos ligados às TIC (-8 pp), os testes de segurança às TIC (-8 pp) ou o controlo de acesso à rede (-9 pp). A medida mais aplicada foi a autenticação através de uma palavra-passe segura (84%). Por sua vez, uma medida tão importante como o múltiplo fator de autenticação foi aplicada apenas por 28% das empresas em Portugal e 31% na média da UE .

 Tabela 1

MEDIDAS DE SEGURANÇA DAS TIC UTILIZADAS NAS EMPRESAS (%)

	Portugal 2022 (variação 2019 pp)	UE 2022 (variação 2019 pp)
Autenticação através de métodos biométricos para aceder aos sistemas TIC da empresa	12 (-3)	14 (+4)
Autenticação baseada na combinação de pelo menos dois mecanismos de autenticação	28 (N/A)	31 (N/A)
Encriptação de dados, documentos ou mensagens de correio eletrónico	33 (-6)	37 (-1)
Avaliação dos riscos ligados às TIC	33 (-8)	32 (-1)
Testes de segurança às TIC	35 (-8)	35 (-1)
Sistema de monitorização da segurança das TIC que permite detetar atividades suspeitas nos sistemas de TIC e alertar a empresa	41 (N/A)	41 (N/A)
VPN (Rede Virtual Privada)	44 (+2)	49 (+6)
Conservação de ficheiros de registo (histórico) que permitem a análise após incidentes de segurança das TIC	54 (-4)	45 (-1)
Controlo de acesso à rede	63 (-9)	65 (=)
Backup de informação em local distinto	74 (=)	78 (+2)
Autenticação através de uma palavra-passe segura	84 (-1)	82 (+6)

Fonte: Eurostat, 2023e

As atividades relacionadas com a segurança das TIC nas empresas em Portugal em 2022 foram realizadas com uma presença predominante de fornecedores externos (72%), em lugar de pessoal da empresa ou de empresas do grupo (41%). Uma proporção próxima da média da UE.

Tabela 2

TIPO DE PESSOAL NAS EMPRESAS QUE REALIZOU AS ATIVIDADES RELACIONADAS COM A SEGURANÇA DAS TIC (%)

	Portugal 2022 (variação 2019 pp)	UE 2022 (variação 2019 pp)
Pessoal da empresa ou de empresas do grupo	41 (-6)	39 (-1)
Fornecedores externos	72 (-4)	68 (+3)

Fonte: Eurostat, 2023e

A maioria das empresas em Portugal possuia recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC em 2022 (54%), o que representa uma subida de 26 pp relativamente a 2019 e mais 17 pp do que a atual média da UE.

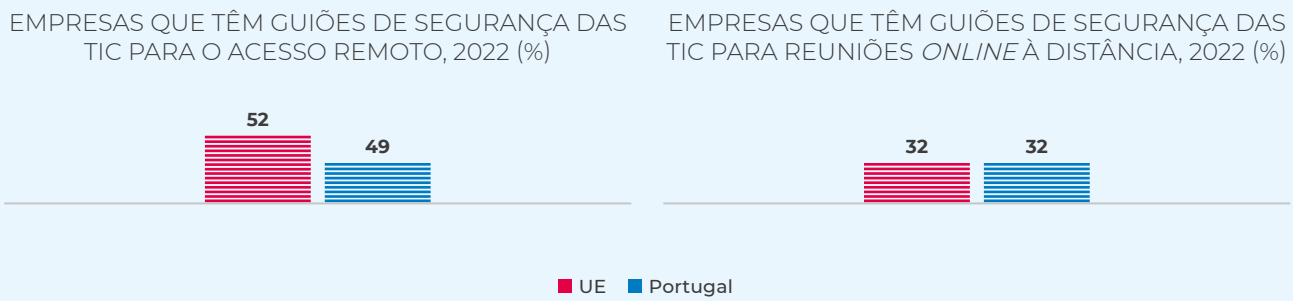
Figura 17

EMPRESAS QUE TÊM RECOMENDAÇÕES DOCUMENTADAS SOBRE MEDIDAS, PRÁTICAS OU PROCEDIMENTOS DE SEGURANÇA DAS TIC, EM PORTUGAL (%)

Fonte: Eurostat, 2023e

Por sua vez, 49% das empresas em Portugal em 2022 tinham guiões de segurança das TIC para o acesso remoto, menos 3 pp do que a média da UE, e 32% tinham guiões de segurança das TIC para reuniões *online* à distância, o mesmo valor do que a média da UE. Estas práticas são particularmente relevantes em contextos de trabalho remoto e híbrido.

Figura 18



Fonte: Eurostat, 2023f e 2023g

DESTAQUES

- Havia mais empresas em Portugal em 2022 com Política de Segurança das TIC definida e revista nos últimos 24 meses (43%) do que a média da UE (32%).
- A medida de segurança das TIC mais aplicada pelas empresas em Portugal em 2022 foi a autenticação através de uma palavra-passe segura (84%).
- Apenas 28% das empresas em Portugal em 2022 aplicou o múltiplo fator de autenticação.
- Os fornecedores externos estavam presentes na maioria (72%) das atividades relacionadas com a segurança das TIC realizadas nas empresas em Portugal, em 2022.
- Mais de metade das empresas em Portugal (54%) tinha recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC em 2022, valor acima da média da UE (37%).
- Menos de metade das empresas em Portugal em 2022 disponibilizou guiões de segurança das TIC para o acesso remoto (49%) ou para reuniões *online* à distância (32%).

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

CIBERSEGURANÇA NA ADMINISTRAÇÃO PÚBLICA

Os Inquéritos à Utilização das TIC na Administração Pública Central e Regional[12] e nas Câmaras Municipais, realizados pela DGEEC (2023a e 2023b), permitem obter uma visão anual sobre as atividades ligadas

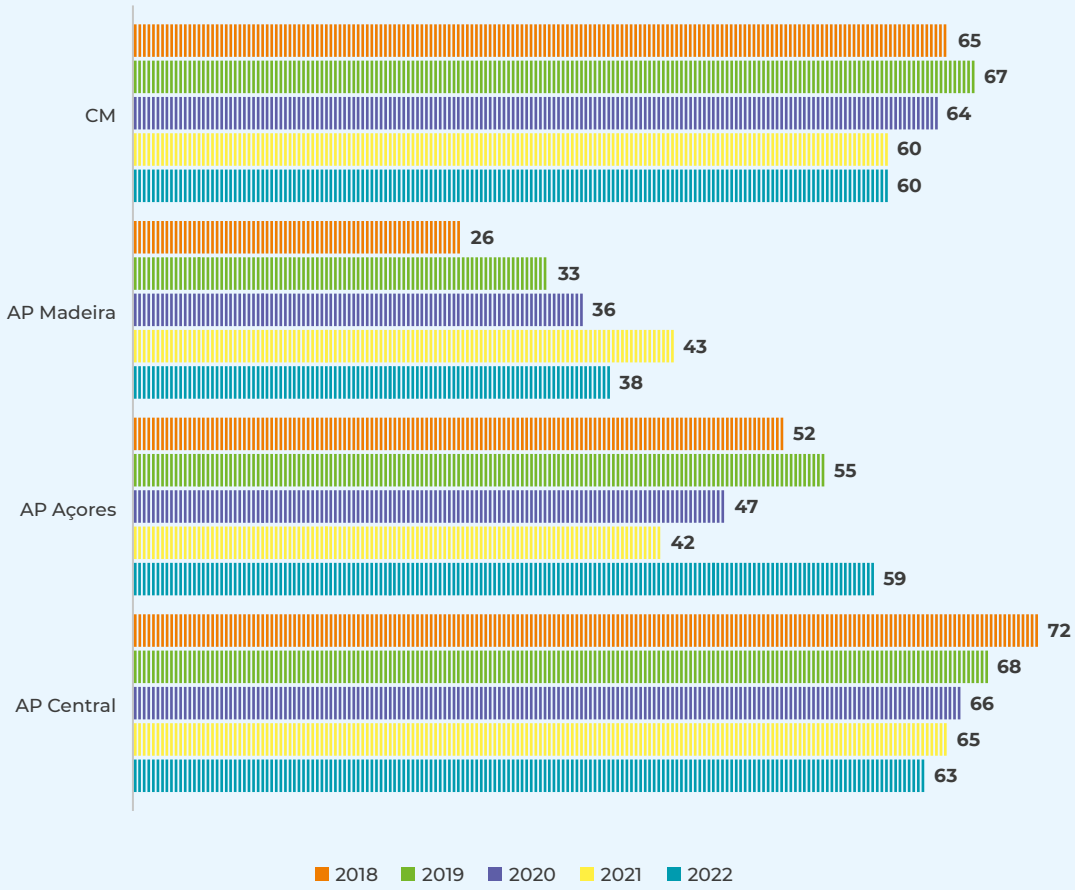
12. "Organismos da Administração Central (exceto fundos de segurança social), constituídos em pessoas coletivas, com exceção das empresas públicas sob controlo de uma unidade da Administração Central ou Regional, Universidades, Estabelecimentos de ensino, Estabelecimentos hospitalares e estruturas temporárias" (DGEEC, 2023a).

à cibersegurança no setor público, fonte a que o presente relatório recorreu em todas as suas edições, havendo uma colaboração na conceção das perguntas por parte do CNCS. Estes inquéritos são realizados a todo o universo em causa e são de resposta obrigatória.

A percentagem de entidades da Administração Pública com uma Estratégia para a Segurança de Informação definida[13] diminuiu na Administração Regional da Madeira (-5 pp) e na Administração Pública Central (-2 pp). Por outro lado, aumentou na Administração Regional dos Açores (+17 pp).

Figura 19

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



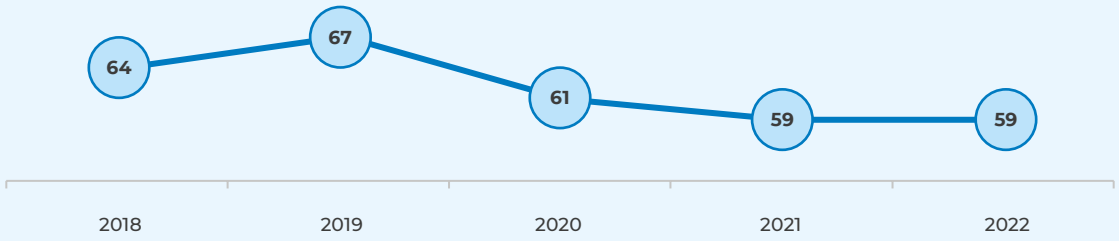
Fonte: DGEEC, 2023a e 2023b

No seu conjunto, em 2022, a percentagem de organismos da Administração Pública com uma Estratégia para a Segurança de Informação definida manteve-se em 59%, tal como no ano anterior.

13. 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 20

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



Fonte: DGEEC, 2023a e 2023b

A Área Metropolitana de Lisboa foi a região com mais Câmaras Municipais com uma Estratégia de Segurança de Informação definida, em 83% destes organismos. A Região Autónoma da Madeira surgiu como a segunda região com mais Câmaras Municipais com este instrumento, com um aumento de 18 pp relativamente ao ano anterior, fixando-se em 73%.

Tabela 3

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

	2022 (variação 2021 pp)
Norte	66 (-5)
Centro	58 (+2)
Área Metropolitana de Lisboa	83 (-6)
Alentejo	47 (+2)
Algarve	63 (-6)
Região Autónoma dos Açores	53 (+11)
Região Autónoma da Madeira	73 (+18)

Fonte: DGEEC, 2023a e 2023

A medida de segurança das TIC mais utilizada em 2022 na Administração Pública em Portugal foi a atualização regular do *software*. Verificou-se ainda uma subida significativa na aplicação de testes de segurança às TIC na Administração Regional dos Açores (+19 pp) e uma descida significativa da autenticação do utilizador através de métodos biométricos na Administração Regional da Madeira (-60 pp). Entre os indicadores analisados pela primeira vez na edição deste ano, destacaram-se com maior frequência de aplicação a realização de inventário de todos os ativos essenciais para a prestação dos serviços de segurança das TIC e a existência de sistema de monitorização da segurança das TIC que permite detetar atividades suspeitas nos sistemas de TIC. O múltiplo fator de autenticação, à exceção da Região Autónoma dos Açores, é aplicado por menos de metade dos organismos.

Tabela 4

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

	AP Central 2022 (variação 2021 pp)	AP Açores 2022 (variação 2021 pp)	AP Madeira 2022 (variação 2021 pp)	CM 2022 (variação 2021 pp)
Atualização regular do *software*	95 (-1)	100 (=)	90 (-10)	98 (-1)
Controlo de acessos à rede do Organismo	92 (+1)	98 (+2)	83 (-17)	96 (+8)
Autenticação dos utilizadores através de uma palavra-passe segura	77 (-9)	98 (+2)	88 (-12)	78 (-5)
Conservação de registos para análise depois da ocorrência de incidentes de segurança	79 (=)	79 (+12)	71 (-8)	76 (+2)
Técnicas de encriptação de dados, documentos e/ou *email**	55 (+4)	52 (+3)	57 (-41)	48 (-5)
Testes de segurança às TIC	63 (+9)	66 (+19)	69 (+3)	52 (+1)
Análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas*	64 (+4)	61 (+12)	62 (-4)	57 (+9)
Autenticação do utilizador através de métodos biométricos*	30 (-3)	32 (-8)	36 (-60)	35 (-11)
Autenticação baseada na combinação de pelo menos dois mecanismos de autenticação**	43	88	47	32
Inventário de todos os ativos essenciais para a prestação dos serviços de segurança das TIC**	77	75	62	77
Cópias de segurança cumprindo a regra 3-2-1**	46	50	50	54
Sistema de monitorização da segurança das TIC que permite detetar atividades suspeitas nos sistemas de TIC**	57	71	72	52

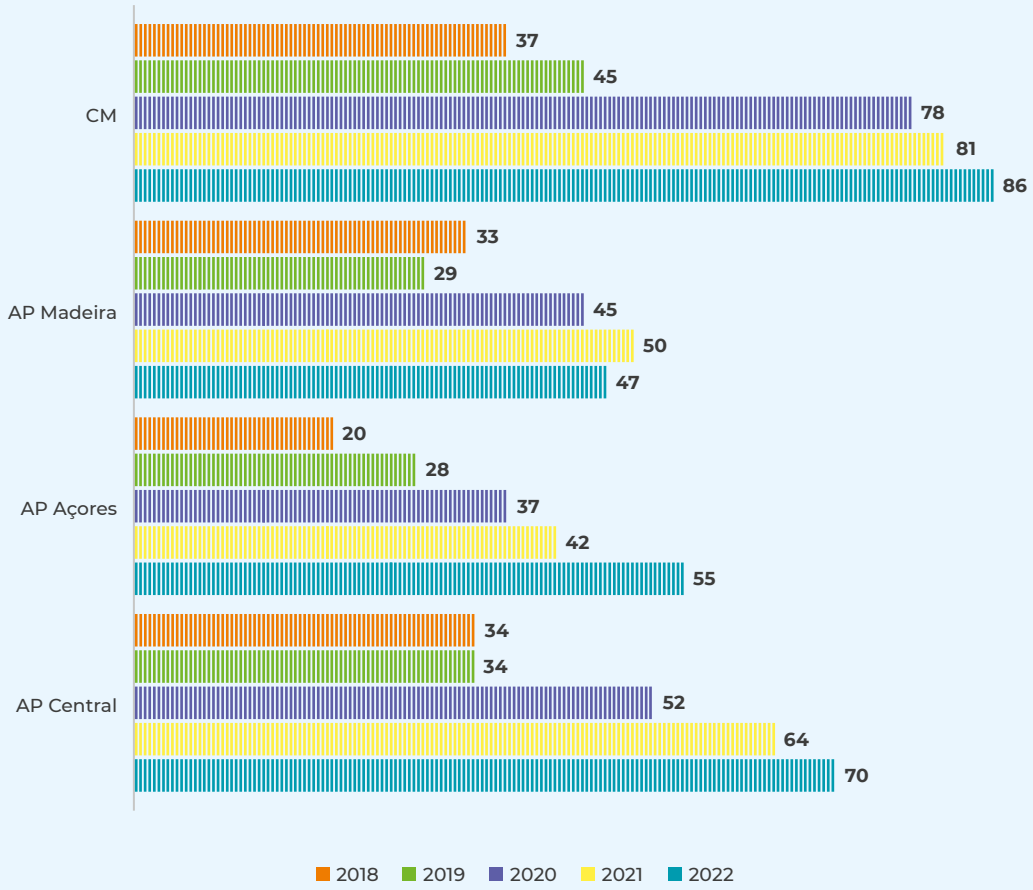
Fonte: DGEEC, 2023a e 2023b

*Texto alterado ligeiramente relativamente ao ano anterior.
**Novo indicador.

A necessidade de reforço de competências em segurança das TIC continua muito elevada na Administração Pública, nomeadamente para 86% das Câmaras Municipais e para 70% da Administração Pública Central.

Figura 21

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

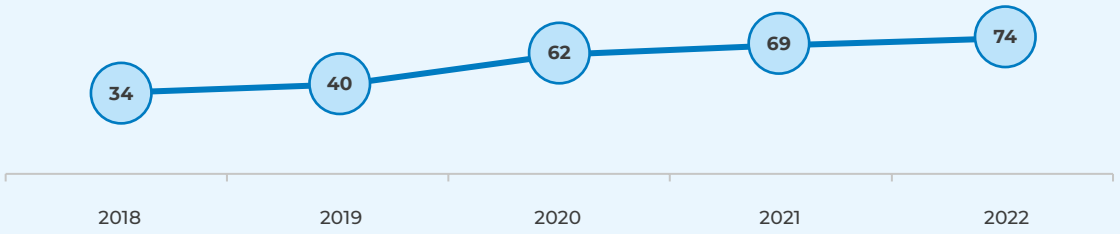


Fonte: DGEEC, 2023a e 2023b

Verificou-se um aumento de 5 pp na percentagem de organismos da Administração Pública no seu conjunto com uma necessidade elevada de reforço de competências em segurança das TIC, passando-se de 69% em 2021 para 74% em 2022. Este valor aumenta de forma constante pelo menos desde 2018.

Figura 22

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, 2023a e 2023b

O Norte e o Alentejo são as regiões nas quais existem mais Câmaras Municipais a manifestar ter uma elevada necessidade de reforço de competências em segurança das TIC, com 91% e 90%, respetivamente. A percentagem de Câmaras Municipais da Região Autónoma da Madeira a manifestarem este nível de necessidade aumentou significativamente, em 28 pp, fixando-se nos 73%.

Tabela 5

PROPORÇÃO DE CÂMARAS MUNICIPAIS QUE INDICARAM TER ELEVADA NECESSIDADE DE REFORÇO DE COMPETÊNCIAS EM SEGURANÇA DAS TIC, POR REGIÃO, EM PORTUGAL, EM 2022, NUTS II (%)

	2022 (variação 2021 pp)
Norte	91 (+11)
Centro	86 (+1)
Área Metropolitana de Lisboa	89 (=)
Alentejo	90 (+6)
Algarve	81 (=)
Região Autónoma dos Açores	68 (-6)
Região Autónoma da Madeira	73 (+28)

Fonte: DGEEC, 2023a e 2023b

CORRELAÇÃO ENTRE ESTRATÉGIAS E NECESSIDADES DE COMPETÊNCIAS NAS CÂMARAS MUNICIPAIS

Analisando os dados das Câmaras Municipais à luz da NUTS III, que permite uma comparação mais fina, é possível avaliar se existem correlações entre a existência de Estratégias para a Segurança de Informação definidas e a necessidade elevada de competências em segurança das TIC no poder local. A este respeito, os resultados mostram uma tendência para haver alguma correlação negativa entre estes dois aspetos, isto é, quanto mais Estratégias para a Segurança de Informação definidas, menos necessidade elevada de competências em segurança das TIC. Através do coeficiente de correlação de Pearson[14] (que estipula que uma correlação negativa máxima se expressa em "-1" e positiva máxima em "+1", sendo que "0" corresponde a uma não correlação), constata-se que existe uma correlação negativa moderada no conjunto das várias regiões NUTS III (-0,5)[15]. Não obstante, considerando as sub-regiões (NUTS III) integradas nas regiões (NUTS II) isoladamente, esta correlação negativa atinge o valor máximo no Alentejo (-1), seguindo-se o Centro (-0,8) e o Norte (-0,6)[16]. Em 2021, estas correlações negativas eram mais fracas do que em 2022.

Na Administração Pública, ao contrário das empresas, as atividades relacionadas com a segurança das TIC foram realizadas principalmente por pessoal do próprio organismo e menos por fornecedores externos. Esta situação foi inversa nas Câmaras Municipais, o tipo de organismo que manifestou ter mais necessidade de competências em segurança das TIC (86%).

Tabela 6

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 2022 (variação 2021 pp)	AP Açores 2022 (variação 2021 pp)	AP Madeira 2022 (variação 2021 pp)	CM 2022 (variação 2021 pp)
Pessoal do próprio Organismo (apenas)	40 (=)	50 (-1)	45 (-1)	33 (-8)
Fornecedores externos (apenas)	16 (-1)	23 (+1)	29 (-10)	5 (+3)
Pessoal do próprio Organismo e fornecedores externos	39 (+1)	27 (+11)	16 (+7)	60 (+5)

Fonte: DGEEC, 2023[a] e 2023

14. Método frequentemente utilizado para medir a correlação linear entre duas variáveis. O seu resultado indica a intensidade e direção da correlação. A correlação negativa entre duas variáveis tem a sua expressão máxima com um coeficiente de -1; a correlação positiva, com um coeficiente de 1; e um coeficiente de 0 indica a ausência de correlação. A correlação não significa necessariamente uma relação de causa-efeito. (Ver: https://www.jstor.org/stable/115794?origin=ads) [consultado a 14/11/2023]

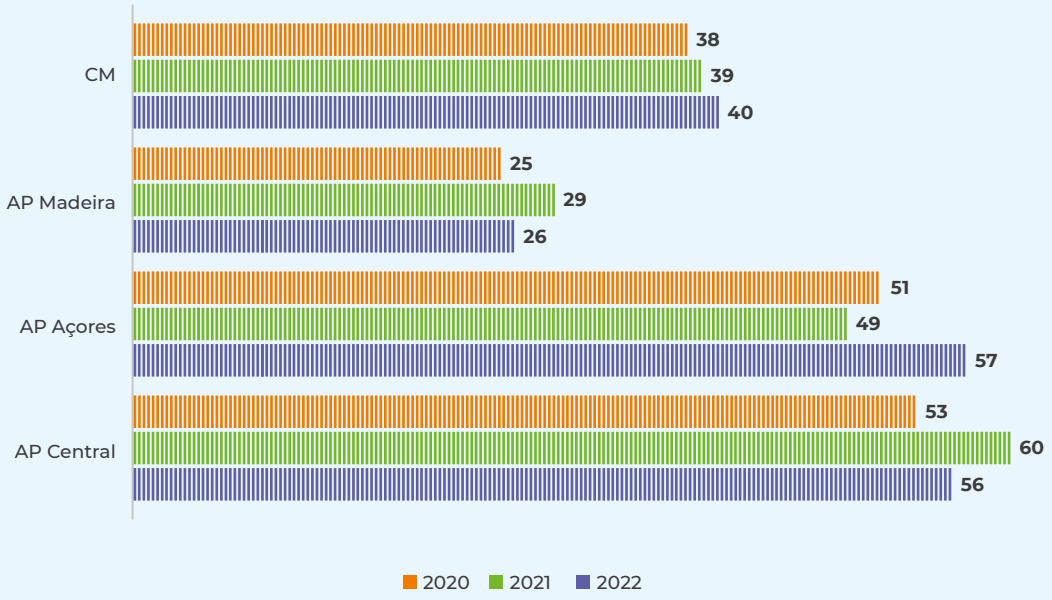
15. Ver posição sobre gradação em que só a partir de 0,5 (negativo ou positivo) se considera haver uma correlação pelo menos moderada: Mukaka, 2012.

16. Nesta análise às sub-regiões da NUTS II não se considerou a Área Metropolitana de Lisboa, o Algarve e as Regiões Autónomas por não terem sub-regiões no âmbito da NUTS III, mas manterem-se as mesmas da NUTS II.

Houve menos organismos com recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC em 2022 face ao ano anterior, na Administração Pública Central, com 56% (-4 pp), e na Administração Regional da Madeira, com 26% (-3 pp). Ao contrário, ocorreu um aumento a este respeito na Administração Regional dos Açores, com 57% (+8 pp), e nas Câmaras Municipais, com 40% (+1 pp).

Figura 23

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



Fonte: DGEEC, 2023a e 2023b

O assunto inscrito nessas recomendações mais frequente, genericamente, em 2022, foi a gestão dos níveis de acesso às TIC. Verificou-se ainda que os procedimentos ou regras para prevenir ou reagir a incidentes de segurança viram a sua presença aumentar 5 pp em ambas as Administrações Regionais.

Tabela 7

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

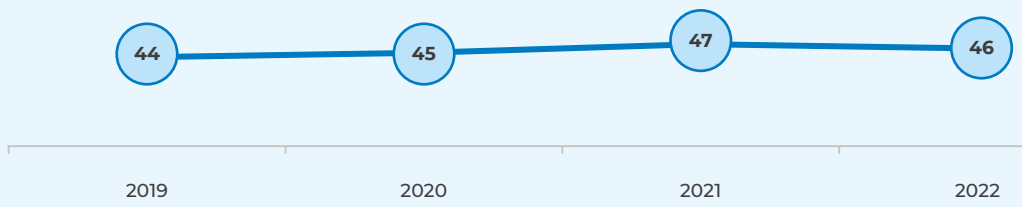
	AP Central 2022 (variação 2021)	AP Açores 2022 (variação 2021)	AP Madeira 2022 (variação 2021)	CM 2022 (variação 2021)
Gestão dos níveis de acesso às TIC	93 (+1)	97 (+8)	100 (+6)	94 (=)
Armazenamento, proteção, acesso e processamento de dados	93 (+2)	88 (-1)	100 (=)	91 (-1)
Responsabilidade, direitos e deveres no que respeita à utilização das TIC	92 (-1)	88 (-5)	87 (-7)	88 (-3)
Procedimentos ou regras para prevenir ou reagir a incidentes de segurança	83 (=)	94 (+5)	93 (+5)	81 (-1)
Formação do pessoal ao serviço para uma utilização segura das TIC	94 (+2)	97 (+4)	93 (-1)	94 (+4)

Fonte: DGEEC, 2023a e 2023b

No conjunto da Administração Pública, ocorreu um ligeiro decréscimo na percentagem de organismos que possuem recomendações documentadas, de 47% para 46% do total, mantendo-se, portanto, num valor inferior a metade dos organismos.

Figura 24

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

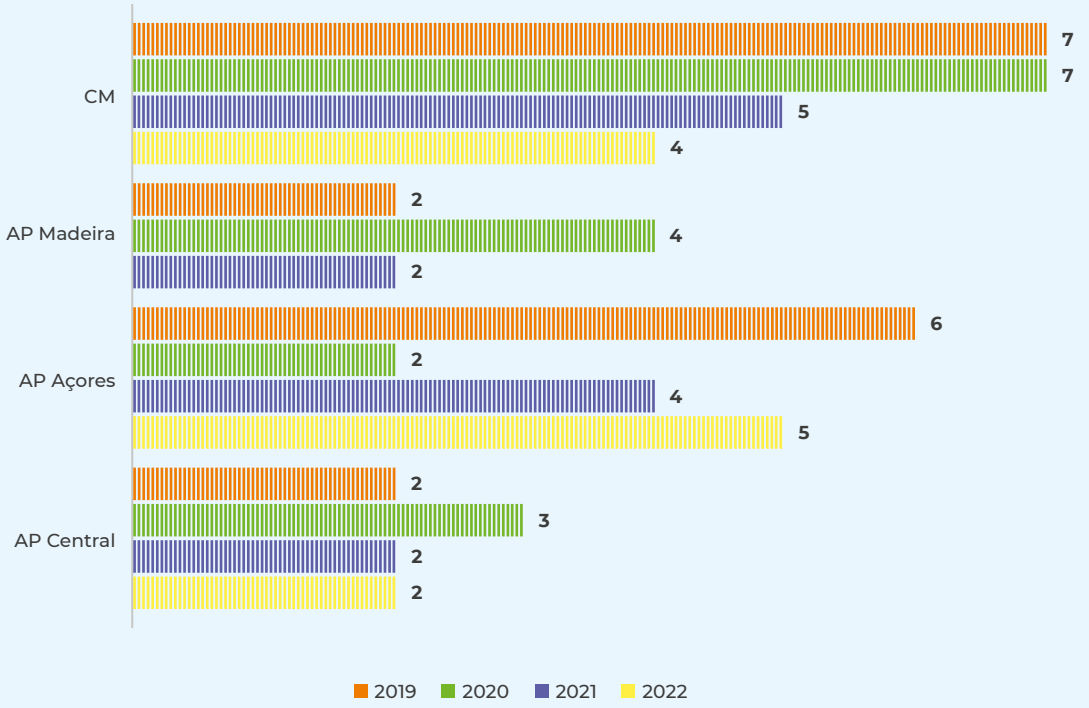


Fonte: DGEEC, 2023a e 2023b

Em 2022, a percentagem de organismos com seguro contra incidentes de segurança das TIC continuou a ser muito residual, tal como se verificou em relação às empresas. Constatam-se mesmo alguns decréscimos face ao ano anterior, como na Administração Regional da Madeira, de 4% para 2%, e nas Câmaras Municipais, de 5% para 4%. A exceção é a Administração Regional dos Açores, na qual se verificou um aumento de 4% para 5%. A Administração Pública Central manteve-se nos 2% de organismos com seguros deste tipo.

Figura 25

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



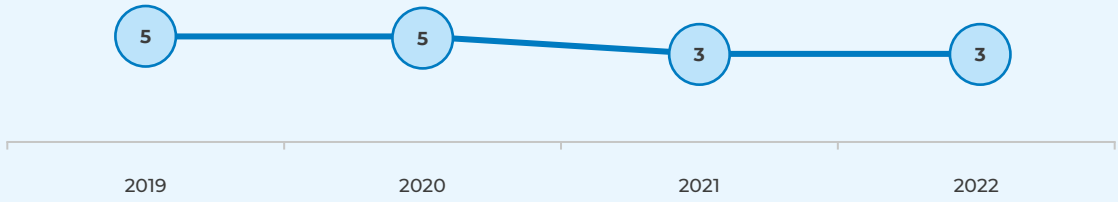
* Relativamente à Administração Regional da Madeira o resultado em 2022 foi considerado nulo pela DGEEC.

Fonte: DGEEC, 2023a e 2023b

No seu conjunto, a percentagem de organismos da Administração Pública com seguro contra incidentes de segurança das TIC estabilizou nos 3% em 2021 e 2022, depois de nos dois anos anteriores se ter mantido nos 5%.

Figura 26

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



Fonte: DGEEC, 2023a e 2023b

DESTAQUES

- A percentagem de organismos da Administração Pública com uma Estratégia para a Segurança de Informação definida manteve-se nos 59% em 2022, tal como no ano anterior.
- A Área Metropolitana de Lisboa foi a região com mais Câmaras Municipais com uma Estratégias para a Segurança de Informação definida, com 83%, em 2022.
- A atualização regular do *software* foi a medida de segurança das TIC mais utilizada na Administração Pública em 2022. Menos de metade aplicou o múltiplo fator de autenticação.
- Tal como em anos anteriores, continuou a aumentar a indicação de haver uma necessidade elevada de competências em segurança das TIC no conjunto da Administração Pública, passando-se de 69% em 2021 para 74% em 2022. As Câmaras Municipais destacaram-se com 86%, com maior incidência no Norte (91%) e no Alentejo (90%).
- No geral, verificou-se que, em 2022, quanto mais as Câmaras Municipais têm Estratégias para a Segurança de Informação definidas menos manifestam necessidade elevada de reforço das competências em segurança das TIC. Este resultado é particularmente evidente nas regiões do Alentejo e do Centro.
- Na Administração Pública, em 2022, predominou o pessoal do próprio organismo a realizar atividades relacionadas com a segurança das TIC, ao contrário do que mostram os resultados relativos às empresas.
- A percentagem de organismos do conjunto da Administração Pública com recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC decresceu de 47% em 2021 para 46% em 2022.
- Apenas 3% dos organismos do conjunto da Administração Pública possuíam seguro contra incidentes de segurança nas TIC, em 2022, tal como no ano anterior.

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

“A QUANTIDADE DE CURSOS DE ENSINO SUPERIOR EM CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO CONTINUA A AUMENTAR.”

F. SENSIBILIZAÇÃO E EDUCAÇÃO

As ações de sensibilização e a educação são instrumentos fundamentais para o desenvolvimento de competências de cibersegurança no cidadão comum e em potenciais especialistas. Neste capítulo, analisam-se dados respeitantes a estas duas dimensões recolhidos pelo Observatório de Cibersegurança do CNCS através de inquérito e de seleção de dados da Direção-Geral do Ensino Superior (DGES) e da DGEEC.

AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA

Mediante a aplicação anual do *Inquérito sobre a Sensibilização para a Cibersegurança em Portugal*, realizado pelo Observatório de Cibersegurança do CNCS, é possível aceder a um conjunto de dados sobre as ações de sensibilização realizadas no país. Este inquérito é dirigido a algumas entidades do universo de colaborações com o CNCS e do âmbito do Centro Internet Segura que realizam este tipo de ações sem fins lucrativos para públicos externos[17]. Sempre que considerado adequado do ponto de vista estatístico, fazem-se comparações com anos anteriores. Os valores recolhidos correspondem sobretudo a estimativas e não a números definitivos.

Em 2022, realizaram-se pelo menos 13 634 ações de sensibilização em cibersegurança no país, considerando sessões presenciais e *online*, cursos *online*, bem como campanhas nas redes sociais, *websites*, comunicação social, MUPI, entre outros. As sessões e os cursos *online* alcançaram cerca de um milhão de pessoas e as campanhas quase 7 milhões de visualizações.

17. Responderam a este inquérito as seguintes entidades: AEPDV - Associação das Empresas Produtoras e Distribuidoras de Videojogos; ANACOM - Autoridade Nacional de Comunicações; APDSI - Associação para a Promoção e Desenvolvimento da Sociedade da Informação; Associação DNS.PT (.PT); AP2SI - Associação Portuguesa para a Promoção da Segurança da Informação; Centro Nacional de Cibersegurança; DICAD - Divisão de Intervenção nos Comportamentos Aditivos e nas Dependências (ARS Norte IP); FGE - Direção-Geral da Educação (Centro de Sensibilização SeguraNet); IAPMEI - Agência para a Competitividade e Inovação, I.P.; INCoDe.2030; Rede de Bibliotecas Escolares (Ministério da Educação); Santa Casa da Misericórdia de Lisboa.

Tabela 8

AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA REALIZADAS EM PORTUGAL POR ENTIDADES COM ESSA MISSÃO SELECIONADAS, PESSOAS ALCANÇADAS PELAS MESMAS E VISUALIZAÇÕES (ESTIMATIVA), 2022

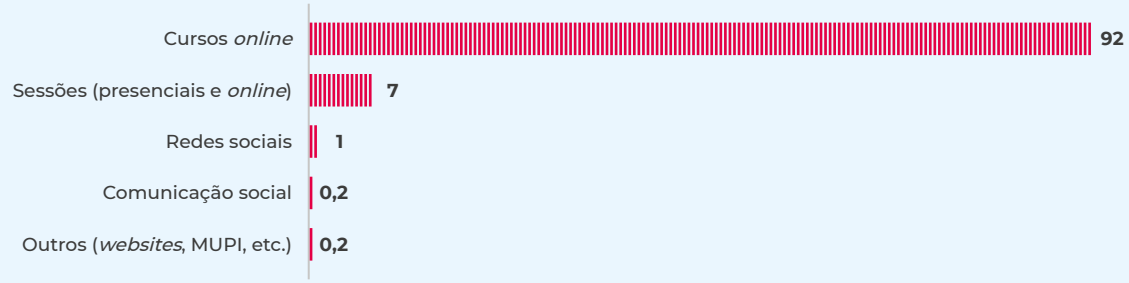
	Nº
Total de ações	13 634
Pessoas alcançadas (sessões presenciais e *online* e cursos *online*)	1 066 569
Visualizações (redes sociais, *websites* e outros)	6 742 476

Fonte: CNCS

Proporcionalmente, os cursos *online* foram o tipo de ação dominante, correspondendo a 92% das ações realizadas. Esta situação deveu-se sobretudo ao facto de que, no âmbito da atividade do Centro de Sensibilização SeguraNet da DGE, ter sido desenvolvida uma grande diversidade de cursos *online* dirigidos a grupos de alunos, cada curso com conteúdos específicos, contabilizando-se por essa via cerca de 12 mil cursos diferentes. Seguem-se, em termos de quantidade de ações, as sessões de sensibilização presenciais e *online* (7%) e as campanhas nas redes sociais (1%). Com um número de ações residuais, surgem as redes sociais e as restantes categorias.

Figura 27

PROPORÇÕES DE AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA POR TIPO REALIZADAS EM PORTUGAL POR ENTIDADES COM ESSA MISSÃO SELECIONADAS (ESTIMATIVA), 2022 (%)

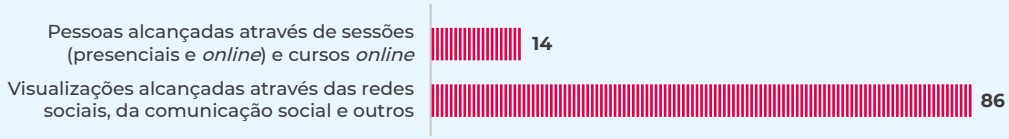


Fonte: CNCS

O número de visualizações não corresponde ao número de pessoas alcançadas. No entanto, pode afirmar-se que se verifica um maior alcance no que diz respeito às redes sociais, comunicação social e outros meios, por via de visualizações, do que nas sessões e cursos *online*, por via de pessoas alcançadas, ainda que as sessões e os cursos compreendam um maior número de ações. Deve considerar-se, contudo, que há mais envolvimento do público-alvo nas sessões e nos cursos do que nos restantes meios.

Figura 28

PROPORÇÃO DE PESSOAS ALCANÇADAS E VISUALIZAÇÕES NAS AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA REALIZADAS EM PORTUGAL POR ENTIDADES COM ESSA MISSÃO SELECIONADAS (ESTIMATIVA), 2022 (%)

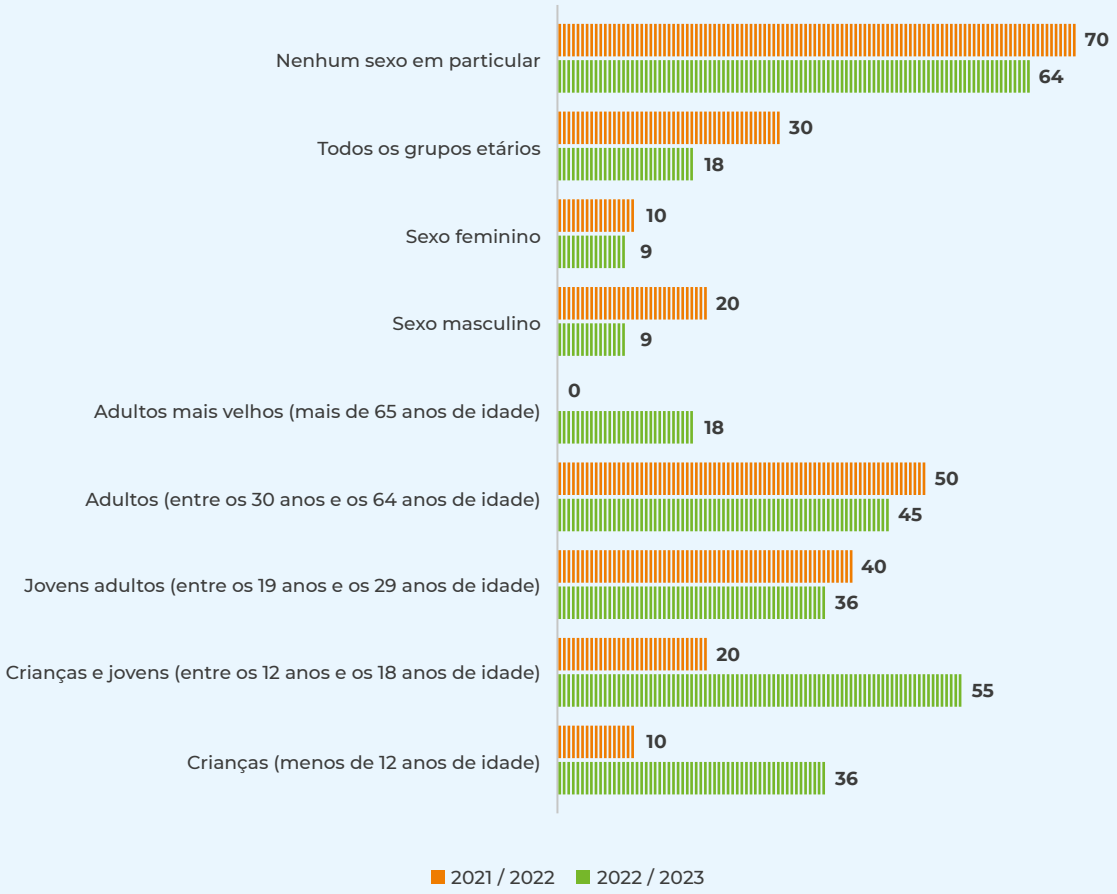


Fonte: CNCS

Comparativamente com o ciclo anterior, em 2022/2023 continuou a não ser privilegiado um sexo específico em termos de público-alvo. Contudo, no que se refere a idades, verificou-se um claro aumento das ações dirigidas a crianças e jovens até aos 18 anos, bem como, em termos relativos, uma maior aposta em ações dirigidas a adultos mais velhos.

Figura 29

CARACTERIZAÇÃO POR SEXO E IDADE DO PÚBLICO-ALVO PREDOMINANTE NAS AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA REALIZADAS POR ENTIDADES COM ESSA MISSÃO SELECIONADAS (ESTIMATIVA), EM PORTUGAL (%)*



* Múltiplas respostas possíveis. Os valores referentes a 2023 compreendem apenas o 1º semestre.

Fonte: CNCS

O tema mais tratado nas ações de sensibilização em 2022 e 2023 (até ao 1º semestre) foi o de boas práticas genéricas de ciber-higiene, em quase metade das organizações, seguindo-se a proteção de dados, privacidade e direitos e o *cyberbullying*.

Tabela 9

TEMAS TRATADOS NAS AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA REALIZADAS EM PORTUGAL, POR ENTIDADES COM ESSA MISSÃO SELECIONADAS, EM 2022/2023 (%)*

Boas práticas genéricas de ciber-higiene	45
Proteção de dados, privacidade e direitos	36
Cyberbullying	18
Riscos *online* e *cibercrime*	9
Gestão da cibersegurança e empresas	9
Prevenção de dependência e bem-estar *online*	9
Cuidados nas redes sociais	9
Componente tecnológica da cibersegurança	9

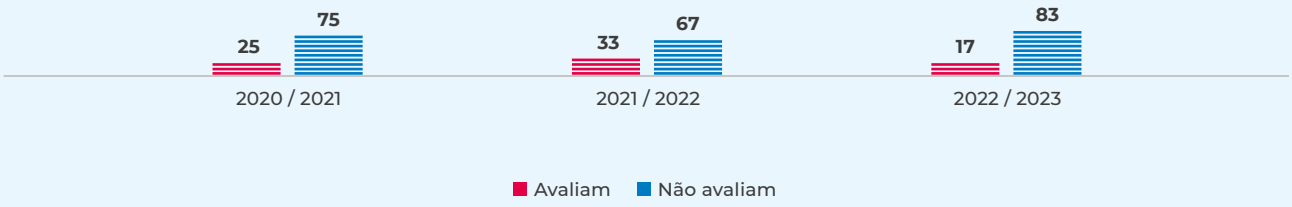
Fonte: CNCS

*Múltiplas respostas possíveis. Os valores referentes a 2023 compreendem apenas o 1º semestre.

A percentagem de entidades que não avalia o impacto das ações de sensibilização em cibersegurança continua a ser muito elevada (83%), tendo mesmo aumentado relativamente ao período anterior (+16 pp). Contudo, as entidades que o fazem são as que realizam mais ações e com mais alcance. Esta avaliação refere-se à análise de eventuais mudanças de comportamento positivas resultantes das ações e não meramente à satisfação com as estratégias ou os conteúdos utilizados por parte dos utilizadores.

Figura 30

ENTIDADES SELECIONADAS QUE UTILIZARAM ALGUM MECANISMO DE AVALIAÇÃO DE IMPACTO DAS AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA REALIZADAS EM PORTUGAL (%)*



* As entidades que realizam análises de impacto são as que fazem mais ações e com maior alcance. Os valores referentes a 2023 compreendem apenas o 1º semestre.

Fonte: CNCS

DESTAQUES

- Em 2022, realizaram-se pelo menos cerca de 13 634 ações de sensibilização em cibersegurança no país e alcançaram-se mais de 1 milhão de pessoas através de sessões presenciais e *online* e de cursos *online*, bem como quase 7 milhões de visualizações em redes sociais, *website* e MUPI.
- A maioria das ações de sensibilização realizadas ocorreram através de cursos *online* (92%).
- Ainda que compreendam um menor número de ações e menos envolvimento do público-alvo do que os cursos *online* e as sessões presenciais e *online*, as campanhas de sensibilização em cibersegurança nas redes sociais, comunicação social, MUPI e outros meios tiveram um alcance bastante elevado no que se refere ao número de visualizações.
- Comparativamente, houve mais ações de sensibilização em cibersegurança dirigidas a crianças e jovens em 2022/2023 do que anteriormente. Em termos de sexo, não existe um predomínio.
- Os temas mais frequentemente tratados nas ações de sensibilização dirigidas a um público externo por entidades que assumem essa missão, em 2022/2023, foram as boas práticas genéricas de ciber-higiene, a proteção de dados, privacidade e direitos e o *cyberbullying*.
- A maioria das entidades que realizaram ações de sensibilização em cibersegurança dirigidas a um público externo não avaliaram o impacto das mesmas no comportamento desse público-alvo (83%). Contudo, as que o fizeram foram as que realizaram mais ações e tiveram mais alcance.

SENSIBILIZAÇÃO NAS EMPRESAS E NA ADMINISTRAÇÃO PÚBLICA

Retomando os dados do Eurostat sobre as práticas de seguranças das TIC nas empresas[18], verifica-se que há uma tendência em 2022 para que aumentem as ações de sensibilização neste domínio dirigidas aos empregados, na medida em que 63% das empresas realizaram ações deste tipo, o que representa um aumento de 9 pp em relação a 2019 e mais 5 pp do que a média da UE. O peso das ações voluntárias aumentou também em comparação com as obrigatórias e as disposições contratuais.

18. Empresas com mais do que 10 empregados, sem contar com o setor financeiro.

Tabela 10

TIPO DE AÇÃO EFETUADA PELAS EMPRESAS JUNTO DO PESSOAL AO SERVIÇO PARA CONSCIENCIALIZAÇÃO DAS SUAS OBRIGAÇÕES EM MATÉRIA DE SEGURANÇA DAS TIC. (%)

	Portugal 2022 (variação 2019 pp)	UE 2022 (variação 2019 pp)
Ações de formação voluntária ou informação interna disponível	56 (+12)	42 (=)
Disposições contratuais	16 (-11)	32 (-5)
Ações de formação obrigatória e/ou consulta obrigatória de informação	19 (-8)	21 (-1)
Consciencialização do pessoal ao serviço	63 (+9)	58 (-3)

Fonte: Eurostat 2023e

No que se refere à Administração Pública, os dados da DGEEC mostram que, embora as ações de sensibilização voluntárias sejam claramente predominantes, verificou-se um crescimento relevante na percentagem de organismos a terem disposições contratuais para os seus empregados ligadas a este tema, como é o caso da Administração Pública Central, com mais 10 pp em 2022 do que no ano anterior, e a Administração Regional dos Açores, com mais 14 pp.

Tabela 11

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* (%)

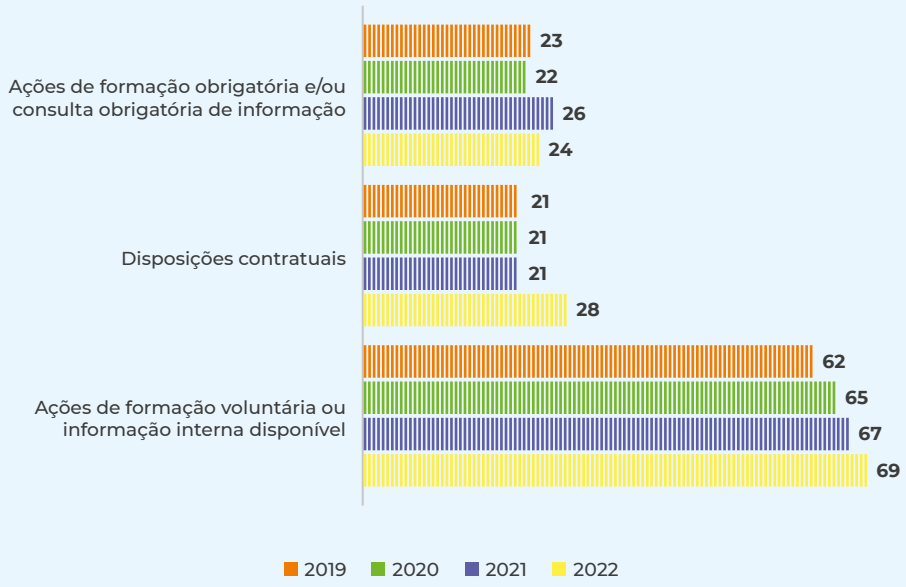
	AP Central 2022 (variação 2021 pp)	AP Açores 2022 (variação 2021 pp)	AP Madeira 2022 (variação 2021 pp)	CM 2022 (variação 2021 pp)
Ações de formação voluntária ou informação interna disponível	73 (-1)	82 (+13)	69 (+1)	64 (+3)
Disposições contratuais	34 (+10)	32 (+14)	19 (+10)	23 (+2)
Ações de formação obrigatória e/ou consulta obrigatória de informação	31 (+1)	25 (+5)	21 (-2)	19 (-4)

FONTE: DGEEC 2023a e 2023b

No conjunto dos organismos da Administração Pública, verificou-se um reforço das disposições contratuais relativas a este tema, com um aumento de 7 pp, de 21% em 2021 (valor que se manteve desde 2019) para 28% em 2022. As ações de formação obrigatórias, contudo, decresceram ligeiramente, de 26% para 24%, enquanto as voluntárias subiram, de 67% para 69% dos organismos.

Figura 31

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



Fonte: DGEEC, 2023a e 2023b

DESTAQUES

- Em 2022, comparando com 2019, houve mais empresas a realizar ações de sensibilização para os seus empregados em matéria de segurança das TIC, fixando-se nos 63%, mais 9 pp.
- Verificou-se um crescimento assinalável na percentagem de organismos da Administração Pública a converterem para disposições contratuais as obrigações em matéria de segurança das TIC dirigidas ao seu pessoal ao serviço, de 21% em 2021 para 28% em 2022.

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

CURSOS DO ENSINO SUPERIOR EM CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO

A quantidade de cursos de ensino superior em cibersegurança e segurança de informação continua a aumentar[19]. Tal como no ano anterior, em 2023 registaram-se mais três cursos. Contudo, enquanto em 2022 houve apenas novos cursos de técnico superior profissional (TESP), em 2023 há mais duas novas licenciaturas e um mestrado, somando 28 cursos no total.

 Tabela 12

CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL, 2023

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	TESP	Universidade de Aveiro - Escola Superior de Tecnologia e Gestão de Águeda
Cibersegurança e Redes informáticas	TESP	Instituto Politécnico de Leiria - Escola Superior de Tecnologia e Gestão
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	TESP	Instituto Politécnico de Viseu - Escola Superior de Tecnologia e Gestão de Lamego
Tecnologias Militares de Segurança – Transmissões, Informática e Eletrónica	TESP	Instituto Universitário Militar - Unidade Politécnica Militar
Engenharia de Redes e Segurança Informática (NOVO)	Licenciatura	Instituto Superior de Tecnologias Avançadas de Lisboa
Segurança Informática em Redes de Computadores	Licenciatura	Instituto Politécnico do Porto - Escola Superior de Tecnologia e Gestão

19. Apenas se consideram os cursos registados na DGES e não outros cursos Executivos e/ou Pós-graduações ministrados no ensino superior. Tal deve-se ao rigor e disponibilidade do tipo de registo assim disponível.

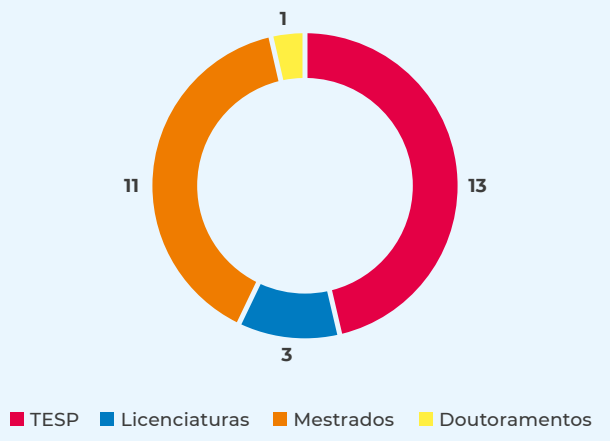
Tecnologias Digitais e Segurança de Informação (NOVO)	Licenciatura	ISCTE - Instituto Universitário de Lisboa (Sintra)
Cibersegurança	Mestrado	Instituto Politécnico de Viana do Castelo - Escola Superior de Tecnologia e Gestão
Cibersegurança	Mestrado	Universidade de Aveiro
Cibersegurança Aplicada (NOVO)	Mestrado	Instituto Politécnico do Cávado e do Ave - Escola Superior de Tecnologia
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

FONTE: DGES (recolha CNCS)

O registo de duas novas licenciaturas fez aumentar o número deste tipo de oferta formativa de uma para três. Uma subida significativa. No entanto, a maioria dos cursos continua a ser TESP (13) e mestrados (11).

Figura 32

CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL POR TIPO/GRAU, 2023

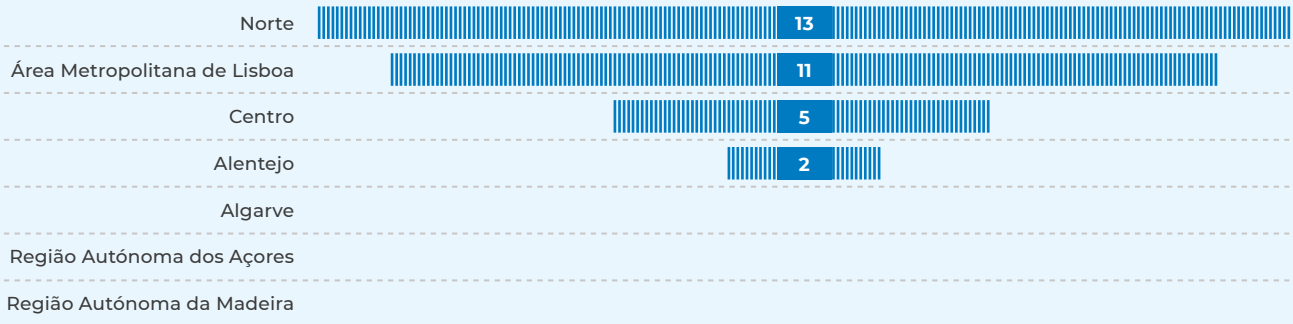


Fonte: DGES (recolha CNCS)

Em termos de distribuição regional, é no Norte que existem mais cursos, quase metade (13), seguindo-se a Área Metropolitana de Lisboa (11), o Centro (5) e o Alentejo (2). As restantes regiões NUTS II - Algarve e Regiões Autónomas - continuam não ter oferta formativa especializada nesta área.

Figura 33

CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL, POR REGIÃO (NUTS II), EM 2023

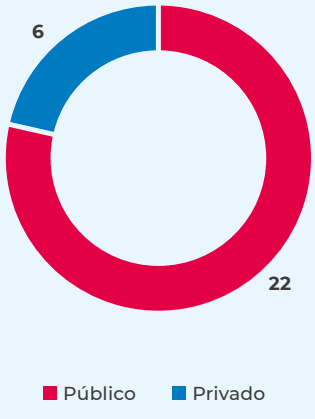


Fonte: DGES (recolha CNCS)

Dos 28 cursos superiores registados, 22 são do ensino público e 6 do ensino privado, o que corresponde a 79% e 21% do total, respetivamente.

Figura 34

NÚMERO DE CURSOS DE ENSINO SUPERIOR EM CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO PÚBLICOS E PRIVADOS EM PORTUGAL, 2023



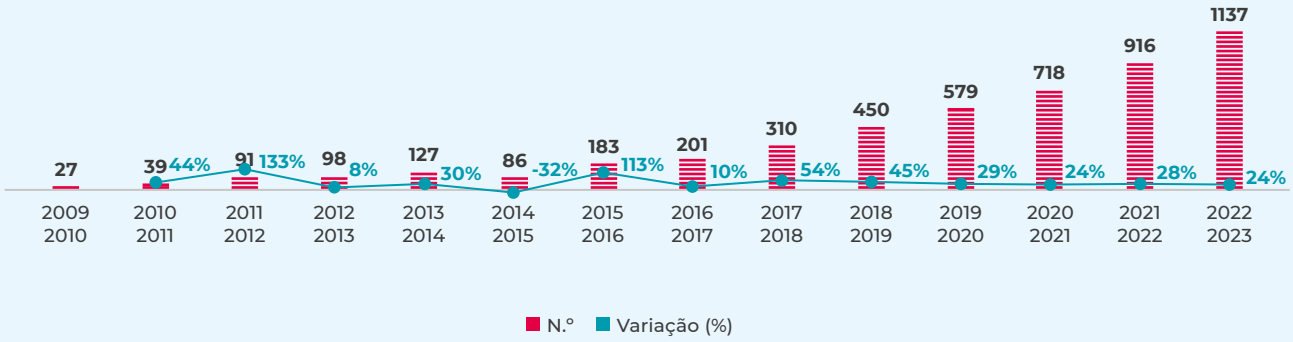
Fonte: DGES (recolha CNCS)

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

O número de alunos inscritos[20] em cursos de ensino superior especializados em cibersegurança e segurança de informação em Portugal continua a aumentar de ano para ano. No ano letivo de 2022/2023, este número aumentou 24%, de 916 no período homólogo para 1137. Este crescimento é contínuo pelo menos deste 2015/2016.

Figura 35

TOTAL DE ALUNOS INSCRITOS EM CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL E VARIAÇÃO ANUAL



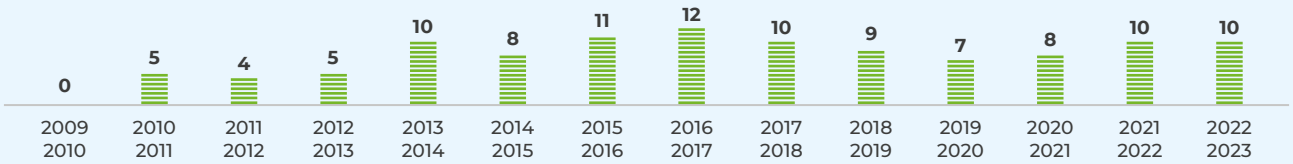
Fonte: DGEEC (recolha CNCS)

A percentagem de mulheres inscritas nestes cursos em 2022/2023 é de 10%, o mesmo valor do ano letivo anterior.

20. "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 36

PERCENTAGEM DE MULHERES INSCRITAS EM CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL (%)

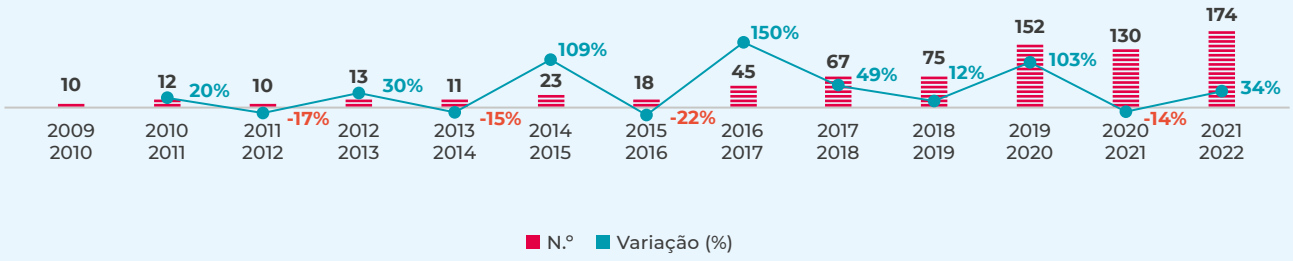


Fonte: DGEEC (recolha CNCS)

O número de alunos diplomados em cursos de cibersegurança e segurança de informação voltou a subir em 2021/2022, desta vez 34%, depois de ter recuado no ano letivo anterior em 14%. O valor total fixou-se em 174 alunos diplomados em 2021/2022, o que equivale a 2,5% dos 6993 alunos diplomados em TIC em 2022 (Pordata) [21].

Figura 37

TOTAL DE ALUNOS DIPLOMADOS EM CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL E VARIAÇÃO ANUAL



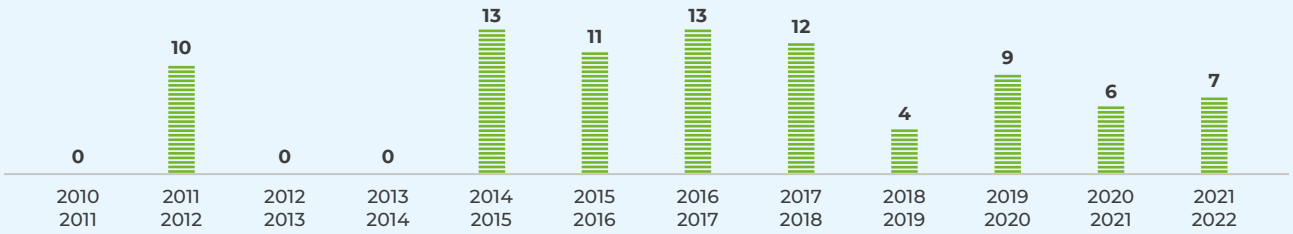
Fonte: DGEEC (recolha CNCS)

A percentagem de mulheres diplomadas subiu 1 pp em 2021/2022, passando para 7% do total, um valor bastante abaixo dos 20,5% de mulheres diplomadas em cursos superiores de TIC em 2022 (Ibid.).

21. Ver Pordata: https://www.pordata.pt/subtema/portugal/sociedade+de+informacao+e+telecomunicacoes-92 [consultado em 03/11/2023]

Figura 38

PERCENTAGEM DE MULHERES DIPLOMADAS EM CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL (%)



Fonte: DGEEC (recolha CNCS)

DESTAQUES

- Em 2023, foram registados mais três cursos do ensino superiores de cibersegurança e segurança de informação em Portugal, nomeadamente duas licenciaturas e um mestrado, somando 28 cursos no total.
- Existem 13 cursos TESP, 11 mestrados, três licenciaturas e um doutoramento em cibersegurança e segurança de informação em Portugal.
- A maioria dos cursos concentra-se no Norte do país e na Área Metropolitana de Lisboa.
- Esta oferta é sobretudo do setor público (79%).
- O número de alunos inscritos em cursos do ensino superior especializados em cibersegurança e segurança de informação aumentou 24%, passando de 916 em 20221/2022 para 1137 em 2022/2023. Destes, apenas 10% são mulheres.
- No ano letivo 2021/2022, o número de diplomados também aumentou, em 34%, passando de 130 no período homólogo para 174, o que equivale a 2,5% do total de diplomados em TIC em 2022. Dos diplomandos em cibersegurança e segurança de informação, 7% são mulheres, abaixo dos 20,5% de mulheres diplomadas em TIC em 2022.

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

“O AUMENTO DE AÇÕES DE SENSIBILIZAÇÃO DIRIGIDAS ÀS CRIANÇAS E JOVENS É UM DADO POSITIVO RELATIVAMENTE À CAPACITAÇÃO DE GRUPOS VULNERÁVEIS.”

G. BRIEFING – ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO

Um dos objetivos do Observatório de Cibersegurança do CNCS é acompanhar os indicadores que possam ter correlação com a execução da ENSC. Não se pretendendo estabelecer relações de causa-efeito entre as medidas da ENSC e estes indicadores, é possível, no entanto, monitorizar o estado da cibersegurança no país e avaliar a sua correspondência ou não com os objetivos da ENSC.

Entre os seis eixos de intervenção da ENSC, o Eixo 2, respeitante a "Prevenção, educação e sensibilização", é diretamente considerável. Ao longo do documento, foram sendo identificadas as medidas deste eixo correlacionadas com os indicadores em análise. Genericamente, estas medidas dividem-se em quatro dimensões.

1. Indicadores relativos à sensibilização do cidadão em geral e das organizações (E2d, E2f e E2r – ver anexo): existe uma elevada variedade de ações de sensibilização em cibersegurança massificadas e com alcance para a população em geral, verificando-se uma tendência para a realização de ações mais dirigidas a públicos e temas específicos, um aspeto que se pode considerar positivo. Menos positivo é o facto de grande parte das organizações que realizam estas ações não sujeitarem estas a avaliações de impacto na mudança de comportamento dos públicos-alvo. Por sua vez, há mais empresas a realizar ações de sensibilização e mais organismos públicos a converter as boas práticas em obrigações contratuais relativamente aos seus empregados.
2. Indicadores relativos à sensibilização de grupos específicos, particularmente vulneráveis (E2e e E2h – ver anexo): o aumento de ações de sensibilização dirigidas às crianças e jovens é um dado positivo relativamente à capacitação de grupos vulneráveis; contudo, no que se refere à formação de especialistas, mantêm-se importantes disparidades entre sexos, com percentagens de mulheres inscritas e diplomadas em cursos do ensino superior de cibersegurança e segurança de informação bastante abaixo do que é comum em cursos TIC.
3. Indicadores relativos à presença da cibersegurança na educação formal (E2g e E2k – ver anexo): persiste uma tendência positiva de aumento do número de cursos de ensino superior especializado em cibersegurança e segurança de informação.

4. Indicadores relativos à qualificação de especialistas (E2l e E2m – ver anexo): o número de inscritos e diplomados em cursos do ensino superior especializado em cibersegurança e segurança de informação continua a aumentar; no entanto, o número de diplomados é ainda residual no contexto dos diplomandos em cursos superiores de TIC em Portugal.

H. RECOMENDAÇÕES

Quadro 2

Aspetos críticos	Recomendações
Maior risco fruto de aumento dos usos da Internet e serviços digitais.	Manter ativas as ações de sensibilização, formação e educação em matéria de cibersegurança junto dos cidadãos em geral.
Insuficiente adoção de Políticas e Estratégias de Segurança de Informação	Continuar a promover, em particular no âmbito do acompanhamento da execução da ENSC, a criação de estratégias e políticas de segurança de informação nas empresas e na Administração Pública. Promover a adoção do Quadro Nacional de Referência para a Cibersegurança.
Aplicação insuficiente de algumas medidas nas organizações (e.g. múltiplo fator de autenticação)	Promover junto das organizações públicas e privadas a adoção das melhores práticas de cibersegurança, nomeadamente através da adoção do Quadro Nacional de Referência para a Cibersegurança e/ou do Selo de Maturidade Digital em Cibersegurança.
Elevada necessidade de competências em segurança das TIC na Administração Pública	Promover a formação, a reconversão e/ou a contratação de pessoal no sentido de uma maior especialização em segurança das TIC na Administração Pública.

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, *Webcheck*, Referencial de Competências em Cibersegurança, Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança, Exercício Nacional de Cibersegurança. **Consultar *website* do CNCS para aceder a estes e outros recursos:** www.cncs.gov.pt

I. NOTAS CONCLUSIVAS

Os resultados apresentados por este documento mostram algumas tendências positivas, como, por exemplo, na educação, mas também aspetos a melhorar, como a crónica falta de recursos humanos na Administração Pública. O objetivo desta análise não é apenas informar, mas também criar condições para melhorar a cibersegurança em Portugal através de metodologias de capacitação das pessoas e das organizações. A seleção de aspetos positivos e negativos tem, pois, como propósito contribuir para o desenvolvimento de conteúdos de sensibilização adequados, a identificação de vulnerabilidades a mitigar nas análises e gestão dos riscos, a definição de estratégias nacionais para a cibersegurança e uma maior precisão na priorização das necessidades.

A posição de Portugal nesta matéria tem evoluído a par de nova legislação, do desenvolvimento e concretização de estratégias e de uma maior notoriedade social do tema. Algumas insuficiências resultam de um grau de exigência maior, mas também das ameaças ao ciberespaço que se normalizam ou emergem. A tensão entre o que se deseja alcançar e as necessidades identificadas correlaciona-se com o nível de ambição na construção de uma sociedade mais ciber-resiliente. O aumento no número e sofisticação dos incidentes de cibersegurança, conjugado com uma maior exposição ao risco por via da crescente presença *online*, os desafios à construção de opinião em democracia colocados por tecnologias como a Inteligência Artificial e um contexto internacional polarizado e conflituoso exigem referenciais de cibersegurança mais ambiciosos. Por isso, a avaliação do estado da cibersegurança em Portugal deve ter em consideração o panorama atual de ameaças ao ciberespaço. Hoje, este panorama exige uma melhoria contínua e um constante renovar de esforços.

J. NOTAS METODOLÓGICAS

A metodologia aplicada no desenvolvimento do presente documento, por um lado, recorre a dados disponíveis em estatísticas públicas e, por outro, recolhe dados através de inquérito e de plataformas abertas. Evitando realizar comparações diretas entre valores não equiparáveis, procura-se, contudo, alimentar séries temporais sobre determinadas temáticas e construir uma visão integrada qualitativa sobre a componente social da cibersegurança, articulando-a com as principais ameaças identificadas noutras análises.

Os dados relativos ao capítulo "Ambiente sociotécnico" foram selecionados de questionários aplicados pelo Eurostat no âmbito do inquérito *ICT usage in households and by individuals, nomeadamente Individuals - internet use* (Eurostat, 2023a), *Individuals - internet activities* (Eurostat, 2023c) e *Internet purchases by individuals* (Eurostat, 2023d). Também do Eurostat, mas no âmbito do inquérito *ICT usage in enterprises*, considerou-se o questionário *Type of connections to the internet by size class of enterprise* (Eurostat, 2023b). Neste capítulo, recorreu-se ainda aos *Inquéritos à Utilização das TIC* aplicados pela DGEEC à Administração Pública Central e Regional, bem como às Câmaras Municipais, dirigidos a todo o universo e não apenas a uma amostra (DGEEC, 2023a e 2023b).

No que se refere ao capítulo sobre o "Interesse pela 'cibersegurança' nos *media* e nas pesquisas *online*", recorreu-se à plataforma Google Trends para recolher e analisar os dados sobre as pesquisas *online* relacionadas com a palavra "cibersegurança" em Portugal, e à plataforma Mediacloud para recolher e analisar o número de artigos publicados nos *media* com o uso deste mesmo termo no país.

Em relação ao capítulo sobre "Atitudes e comportamentos", os dados foram selecionados de duas grandes fontes, em parte já mencionadas: no que diz respeito às empresas, do inquérito *ICT usage in enterprises,* nomeadamente os questionários *Security policy: measures, risks and staff awareness by size class of enterprise* (Eurostat, 2023e), *Remote access by size/class of enterprise* (Eurostat, 2023f) e *Meetings via the internet by size/class of enterprise* (Eurostat, 2023g); no que diz respeito à Administração Pública, dos *Inquéritos à Utilização das TIC* aplicados pela DGEEC à Administração Pública Central e Regional e às Câmaras Municipais (DGEEC, 2023a e 2023b).

Os dados apresentados no capítulo sobre "Sensibilização e educação" são quase na sua totalidade recolhidos pelo CNCS em inquérito e de plataformas abertas, com exceção dos dados referentes às ações de sensibilização nas empresas e na Administração Públicas, ambos recolhidos de fontes já referidas, do Eurostat (2023e) e da DGEEC (2023a e 2023b), respetivamente. A análise apresentada sobre as ações de

sensibilização em cibersegurança dirigidas ao público em geral realizou-se com base em inquérito *online* lançado pelo Observatório de Cibersegurança do CNCS. Este inquérito dirigiu-se a um conjunto de partes interessadas do universo do Centro Internet Segura e do CNCS que assumem responsabilidades na sensibilização da população para o uso seguro da Internet, entre os dias 3 e 15 de novembro de 2023. Obtiveram-se 12 respostas. Os dados sobre os cursos superiores especializados em cibersegurança e segurança de informação foram recolhidos na plataforma de pesquisa por cursos da DGES, recorrendo-se às seguintes palavras-chave: "cibersegurança", "segurança da/e informação", "segurança informática" e "segurança". Para a contabilização do número de alunos e diplomados, considerou-se os mesmos cursos e palavras-chave, mas recorrendo aos dados partilhados pela DGEEC no seu *website*.

Para mais detalhe, consultar as fontes aqui mencionadas através dos *links* indicados nas "Referências principais". Para algum outro esclarecimento adicional, enviar questão para *email* cncs@cncs.gov.pt.

K. ENTIDADES PARCEIRAS NA REALIZAÇÃO DO RELATÓRIO

- **AEPDV** - Associação das Empresas Produtoras e Distribuidoras de Videojogos
- **ANACOM** - Autoridade Nacional de Comunicações
- **AP2SI** - Associação Portuguesa para a Promoção da Segurança da Informação
- **APDSI** - Associação para a Promoção e Desenvolvimento da Sociedade da Informação
- **Associação .PT**
- **COTEC** Portugal - Associação Empresarial para a Inovação
- **DGE** - Direção-Geral da Educação
- **DGEEC** - Direção-Geral de Estatísticas da Educação e Ciência
- **DICAD** - Divisão de Intervenção nos Comportamentos Aditivos e nas Dependências
- **IAPMEI** - Agência para a Competitividade e Inovação, I.P.
- **INCoDe.2030**
- **Rede de Bibliotecas Escolares** (Ministério da Educação)
- **Santa Casa da Misericórdia de Lisboa**

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, 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)

Educação e Sensibilização [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 n.º 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)

- **AEPDV:** Associação das Empresas Produtoras e Distribuidoras de Videojogos.
- **ANACOM:** Autoridade Nacional de Comunicações.
- **AP Açores:** Administração Pública Regional dos Açores.
- **AP Central:** Administração Pública Central.
- **AP Madeira:** Administração Pública Regional da Madeira.
- **AP2SI:** Associação Portuguesa para a Promoção da Segurança da Informação.
- **APAV:** Associação Portuguesa de Apoio à Vítima.
- **APDSI:** Associação para a Promoção e Desenvolvimento da Sociedade da Informação;
- **CM:** Câmaras Municipais.
- **CNCS:** Centro Nacional de Cibersegurança.
- **COTEC [Portugal]:** Associação Empresarial para a Inovação.
- **DGE:** Direção-Geral da Educação.
- **DGEEC:** Direção-Geral de Estatísticas da Educação e Ciência.
- **DGES:** Direção-Geral de Ensino Superior.

- **DICAD:** Divisão de Intervenção nos Comportamentos Aditivos e nas Dependências.
- **DoS/DDoS:** Negação de Serviço/Negação de Serviço Distribuída.
- **DSL:** Linha Digital de Assinante [Digital Subscriber Line].
- **ENSC:** Estratégia Nacional de Segurança do Ciberespaço 2019-2023.
- **IAPMEI:** Agência para a Competitividade e Inovação.
- **INE:** Instituto Nacional de Estatística.
- **MOOC:** Curso Online Aberto e Massivo [Massive Open Online Course].
- **MUPI:** mobiliário urbano para informação.
- **NUTS:** Nomenclatura das Unidades Territoriais para Fins Estatísticos.
- **PME:** Pequenas e Médias Empresas.
- **pp:** pontos percentuais.
- **PT:** Portugal.
- **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 14/11/2023]:

- CNCS (2023) *Relatório Cibersegurança em Portugal – Riscos & Conflitos 2023*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.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-cibersegurana-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 14/11/2023]:

- DGEEC (2023a) *Inquérito à Utilização das Tecnologias da Informação e Comunicação na Administração Pública Central e Regional – IUTICAP 2022*. Direção-Geral de Estatísticas da Educação e Ciência. Disponível em: https://www.dgeec.mec.pt/np4/12.html
- DGEEC (2023b) *Inquérito à Utilização das Tecnologias da Informação e Comunicação nas Câmaras Municipais- IUTICCM 2022*. Direção-Geral de Estatísticas da Educação e Ciência. Disponível em: https://www.dgeec.mec.pt/np4/12.html
- Eurostat (2023a) *Individuals – internet use*. Eurostat. ISOC_CI_IFP_IU. Disponível em: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_ci_ifp_iu
- Eurostat (2023b) *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 (2023c) *Individuals – internet activities*. Eurostat. ISOC_CI_AC_I. Disponível em: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_ci_ac_i
- Eurostat (2023d) *Internet purchases by individuals*. Eurostat. ISOC_EC_IB20. Disponível em: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_ec_ib20

- Eurostat (2023e) *Security policy: measures, risks and staff awareness by size class of enterprise*. ISOC_CISCE_RA. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ra/default/table?lang=en
- Eurostat (2023f) *Remote access by size class of enterprise*. ISOC_CI_RAS. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_ras/default/table?lang=en
- Eurostat (2023g) *Meetings via the internet by size class of enterprise*. ISOC_CI_MVIS. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_mvis/default/table?lang=en

OUTROS DOCUMENTOS

[consultados a 14/11/2023]:

- 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 14/11/2023)

- 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 14/11/2023]:

- https://www.jstor.org/stable/115794?origin=ads
- trends.google.com/trends/?geo=PT
- www.cncs.gov.pt
- www.dgeec.mec.pt
- www.dges.gov.pt/pt/pesquisa_cursos_instituicoes
- www.mediacloud.org/
- www.pordata.pt

ANEXO. LINHAS DE AÇÃO DA ENSC - SOCIEDADE

Quadro 3

	Linhas de Ação do Eixo 2 articuláveis com os indicadores deste relatório	A&C*	S&E
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 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