

DEZEMBRO 2024

RELATÓRIO CIBERSEGURANÇA EM PORTUGAL

SOCIEDADE 2024

6^a EDIÇÃO



FICHA TÉCNICA

Autoria e edição: Centro Nacional de Cibersegurança

Design: Nova Agência

Tiragem: 100 exemplares

ÍNDICE

5	A. Sumário executivo
6	B. Análise global
13	C. Introdução
14	D. Exposição ao digital
14	O uso da Internet
14	Os usos de serviços críticos para a cibersegurança
16	E. Interesse pela “cibersegurança” nos <i>media</i> e nas pesquisas <i>online</i>
16	Número de artigos publicados nos <i>media</i> que mencionaram o termo “cibersegurança”
17	Índice de pesquisas Google com o termo “cibersegurança”
21	F. Atitudes e comportamentos
21	Comportamentos dos indivíduos
22	Competências em cibersegurança nas empresas
24	Cibersegurança na Administração Pública
27	G. Sensibilização e educação
27	Ações de sensibilização em cibersegurança
29	Sensibilização nas empresas e na Administração Pública
30	Cursos do ensino superior em cibersegurança e segurança da informação
32	H. Recomendações
33	I. Notas metodológicas
35	J. Entidades parceiras na realização do relatório
36	K. Termos, siglas e abreviaturas
38	L. Referências principais
41	ANEXO – Linhas de ação da ENSC - Sociedade



HÁ UMA ATITUDE POSITIVA A RESPEITO DA CIBERSEGURANÇA POR PARTE DAS ORGANIZAÇÕES, MAS ESTAS AINDA TÊM FALTA DE RECURSOS INTERNOS



A. SUMÁRIO EXECUTIVO

O presente relatório do Observatório de Cibersegurança faz um acompanhamento anual da vertente social da cibersegurança em Portugal. Para o efeito, analisa as atitudes, os comportamentos e a educação e sensibilização face a esta matéria. A edição deste ano, a sexta, apresenta dados sobretudo de 2023 e alguns de 2024. Este ano optou-se por uma versão mais curta do documento, mas sem sacrificar a abrangência dos dados e a análise.

Esta edição apresenta as seguintes **conclusões** principais:

- Os utilizadores e as organizações têm níveis elevados de exposição aos riscos do ciberespaço, em particular por haver muito uso de certos serviços digitais;
- Algumas ciberameaças ligadas à exploração do fator humano têm índices crescentes de presença em artigos de *media* e, principalmente, nas pesquisas *online*;
- Há uma atitude positiva a respeito da cibersegurança por parte das organizações, mas estas ainda têm falta de recursos internos;
- O alcance das ações de sensibilização é relativamente limitado, nomeadamente por se priorizarem meios de menor abrangência e o contexto organizacional;
- O número de cursos superiores de cibersegurança e segurança da informação, bem como de alunos inscritos e diplomados nos mesmos, continua a aumentar.

Recomendações estratégicas:

- Fazer acompanhar a literacia digital nas escolas e noutros contextos educativos por uma literacia para a cibersegurança,
- Promover de forma mais acentuada boas práticas nas organizações, como o múltiplo fator de autenticação (MFA);
- Capacitar mais os recursos humanos das organizações em cibersegurança, nomeadamente na Administração Pública e pequenas e médias empresas (PME);
- Aumentar o alcance das ações de sensibilização, de modo a atingir um público mais alargado, e desenvolver ações para grupos mais específicos.

O que está bem e deve continuar:

- A consciência da importância da cibersegurança nas organizações, mediante ações tais como a adoção de Estratégias de Segurança da Informação no setor público;
- A tendência das organizações para sensibilizarem mais os seus empregados;
- O investimento das instituições do ensino superior na criação de cursos e na formação de alunos em cibersegurança e segurança da informação.

B. ANÁLISE GLOBAL

De seguida, de forma agregadora, apresenta-se uma síntese das principais conclusões do presente relatório, uma avaliação destes resultados relativamente às ameaças no ciberespaço e um diagnóstico quanto à concretização de algumas das linhas de ação da Estratégia Nacional de Segurança do Ciberespaço (ENSC), com base na análise realizada

TENDÊNCIAS



EXPOSIÇÃO – HÁ UMA ELEVADA EXPOSIÇÃO DIGITAL DOS UTILIZADORES E DAS ORGANIZAÇÕES À INTERNET E A CERTOS SERVIÇOS DIGITAIS

“CONTINUA A HAVER MAIS INDIVÍDUOS EM PORTUGAL A USAR CERTOS SERVIÇOS DIGITAIS DO QUE A MÉDIA DA UNIÃO EUROPEIA.”



Os indivíduos e as organizações mantêm níveis elevados de exposição ao digital, isto é, de conectividade à Internet e a alguns serviços digitais críticos para a cibersegurança. Em particular, continua a haver mais indivíduos em Portugal a usar certos serviços digitais do que a média da União Europeia (UE), nomeadamente *email*, telefonar *online* ou usar chamadas de vídeo *online*, redes sociais e mensagens instantâneas.



SALIÊNCIA DO TEMA – ALGUMAS CIBERAMEAÇAS RELEVANTES LIGADAS AO FATOR HUMANO TÊM SALIÊNCIA CRESCENTE NOS *MEDIA* E NOS ÍNDICES DE PESQUISAS *ONLINE*

O número de artigos nos *media* em Portugal com referências à cibersegurança diminuiu em 2023 face ao ano anterior, contudo, aumentaram as menções a certos tipos de ameaças que foram relevantes, como a *CEO Fraud* e o *spoofing*¹. O interesse relativo pelo termo “cibersegurança” em pesquisas no motor de busca Google aumentou genericamente e manteve-se de forma mais homogénea ao longo dos meses por comparação com 2022. As pesquisas sobre certas ameaças ganharam relevância, como as ligadas a burlas *online*, mostrando, tal como nos artigos dos *media* referidos, uma certa saliência de casos que exploram o fator humano.

1. Para esclarecimento sobre o significado destes e de outros termos, consultar Termos, siglas e abreviaturas.



ATITUDES E COMPORTAMENTOS – AS ORGANIZAÇÕES TÊM SENSIBILIDADE PARA A CIBERSEGURANÇA, MAS CONTAM COM POUCOS RECURSOS INTERNOS

As organizações em Portugal manifestam ter consciência da importância da cibersegurança, dando-lhe relevância e definindo estratégias. Apesar disso, têm poucos recursos internos. Há mais empresas com dificuldade em contratar profissionais na área do que a média da UE e a Administração Pública tem uma elevada necessidade de competências nesta matéria. Talvez por isso, verifica-se uma maior propensão para as organizações contratarem serviços externos de cibersegurança.

Há uma tendência positiva no sentido de os indivíduos verificarem a segurança dos *websites* com os quais partilham os seus dados pessoais e aplicarem outras boas práticas de gestão dos dados pessoais *online*. Em geral, estes cuidados são mais prevalentes nos jovens do que nas pessoas mais velhas.



SENSIBILIZAÇÃO E EDUCAÇÃO – RECORRE-SE POUCO A MEIOS DE GRANDE ALCANCE PARA A REALIZAÇÃO DE CAMPANHAS DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA

A maioria das ações de sensibilização em cibersegurança realizadas por entidades que se dirigem a públicos externos, sem fins lucrativos, em 2023, foram sessões presenciais ou à distância e cursos *online*. As campanhas nas redes sociais e na comunicação social continuaram a ser em número relativamente reduzido, embora tenham mais alcance. Os temas predominantes destas ações de sensibilização foram a cidadania digital, as boas práticas genéricas de ciber-higiene e os cuidados nas redes sociais.

No que diz respeito ao volume de entidades a prestar sensibilização em cibersegurança aos seus empregados, as empresas em Portugal comparam positivamente com a média da UE, mas ainda abaixo do necessário, e a Administração Pública melhorou em todos os indicadores.

O número de cursos, alunos inscritos e diplomados em cursos superiores de cibersegurança e segurança da informação continua a aumentar a um ritmo relativamente elevado.



CENÁRIOS DE AMEAÇAS E O FATOR HUMANO

O Relatório do Observatório de Cibersegurança sobre o tema Riscos & Conflitos, de 2024, destacou as ciberameaças mais relevantes a afetar Portugal em 2023, com tendência a manterem-se em 2024 (CNCS, 2024). Considerando as principais conclusões do presente documento, é importante perceber o que contribui ou não para mitigar essas ciberameaças. O quadro 1 estabelece essa correlação.

No presente relatório identificam-se diversos aspetos sociais que se constituem como fragilidades relativamente às ciberameaças mais relevantes. Por exemplo, um maior uso de certos serviços digitais representa uma exposição ao risco de forma transversal. A dificuldade que as empresas e a Administração Pública têm em internalizar competências especializadas em cibersegurança é negativa para a proteção contra ameaças com um maior pendor técnico, como o *ransomware* e, em parte, o comprometimento de contas. O insuficiente uso do MFA na Administração Pública é particularmente preocupante, atuando negativamente sobre estas e outras ameaças, sobretudo as que envolvem palavras-passe e o acesso a contas. Igualmente negativa é a falta de uma maior massificação das ações de sensibilização em cibersegurança e a quase ausência de avaliação do impacto, nos comportamentos dos públicos-alvo, das ações que são realizadas em geral. Esta situação interfere com a capacidade de as boas práticas de ciber-higiene chegarem a públicos mais alargados e saber se foram efetivamente assimiladas.

Outros aspetos, pelo contrário, mitigam os potenciais efeitos das ciberameaças. É o caso da saliência relativa de temas ligados a ciberameaças que exploram o fator humano em pesquisas no motor de busca Google e em artigos nos *media*, mostrando interesse pela matéria; o cuidado individual com a segurança dos *websites* com que os utilizadores partilham os seus dados pessoais, tantas vezes usados em ataques que usam engenharia social; os níveis crescentes de alerta para a cibersegurança por parte das empresas e de Estratégias para a Segurança da Informação definidas pela Administração Pública, melhorando a capacitação destas entidades; o aumento de algumas boas práticas na Administração Pública, como o inventário de ativos, o controlo de acessos e o registo de *logs*, favorecendo a proteção e a recuperação de incidentes; a diversidade de temas tratados nas ações de sensibilização dirigidas ao público em geral, promovendo competências transversais; o crescimento no número de entidades a sensibilizar os seus colaboradores, reforçando o fator humano; e o aumento do número de cursos superiores de cibersegurança e segurança de informação, bem como de inscritos e diplomados, proporcionando a formação de mais especialistas.



RELAÇÃO ENTRE RESULTADOS DESTE RELATÓRIO E PRINCIPAIS AMEAÇAS AO CIBERESPAÇO DE INTERESSE NACIONAL, EM 2023/2024

Resultados de Sociedade 2024 / Ciberameaças em Riscos e Conflitos 2024 (CNCS, 2024)	Ransomware	Phishing/ Smishing	Engenharia Social	Burlas Online	Comprometimento de conta
Elevado risco devido ao número alto de indivíduos a usar plataformas digitais críticas para a cibersegurança					
Elevado risco em resultado de haver muitas organizações com ligação à Internet					
Aumento das pesquisas <i>online</i> relacionadas com a cibersegurança, em particular sobre fraudes que exploram o fator humano (algumas mais mencionadas em artigos nos <i>media</i>)					
Há mais indivíduos em Portugal do que a média da UE a verificar se os <i>websites</i> a que os seus dados pessoais são fornecidos são seguros					
A maioria das empresas considera que a cibersegurança é uma prioridade bastante alta ou muito elevada					
Há mais empresas em Portugal do que a média da UE a ter dificuldades em encontrar e contratar profissionais com competências em cibersegurança					
Apenas cerca de 1 em cada 10 empresas em Portugal tem trabalhadores diretamente envolvidos em cibersegurança com certificações na área ou a trabalhar para as obter. A média da UE é de 2 em cada 10					
Há mais organismos da Administração Pública com uma estratégia para a segurança da informação definida, atingindo cerca de 7 em cada 10					
O volume de organismos da Administração Pública a usar MFA decresceu para menos de metade					
Há um crescimento significativo do volume de organismos da Administração Pública a realizar inventário de ativos, a ter controlo de acessos e a conservar os <i>logs</i>					



Resultados de Sociedade 2024 / Ciberameaças em Riscos e Conflitos 2024 (CNCS, 2024)	Ransomware	Phishing/Smishing	Engenharia Social	Burlas Online	Comprometimento de conta
O volume de organismos da Administração Pública com elevada necessidade de reforço de competências em cibersegurança mantém-se muito elevado, em cerca de 7 em cada 10 organismos; nas câmaras municipais, atinge-se os 9 em cada 10					
Verifica-se um aumento, para mais de metade, no volume de organismos da Administração Pública com recomendações documentadas sobre medidas, práticas ou procedimentos de cibersegurança disponibilizadas					
A maioria das ações de sensibilização em cibersegurança realizadas a públicos externos por organizações com essa missão não utiliza a comunicação social ou outros meios de maior alcance					
Os temas mais tratados nas ações de sensibilização dirigidas a públicos externos foram a cidadania digital, as boas práticas genéricas de ciber-higiene e os cuidados nas redes sociais					
A maioria das organizações que fazem ações de sensibilização para públicos externos não avaliam os resultados nos comportamentos do público-alvo					
Um pouco mais de um quarto das empresas em Portugal fornece formação ou consciencialização sobre cibersegurança aos seus funcionários, ligeiramente acima da média da UE					
O volume de organismos da Administração Pública a realizar ações de sensibilização aumentou, atingindo cerca de 7 em cada 10 no que diz respeito às ações voluntárias					
O número de cursos superiores de cibersegurança e segurança da informação aumentou de 29 para 37, bem como o número de alunos e diplomados					

Fonte: CNCS

- Não contribui para a mitigação da ameaça
- Contribui para a mitigação da ameaça
- Sem relevância significativa

ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO 2019-2023 (ENSC)

O ciclo de vida da ENSC terminou, mas não a necessidade de avaliar os seus potenciais efeitos, ainda que evitando estabelecer correlações diretas entre determinadas linhas de ação da ENSC e os indicadores apresentados. A temática tratada neste estudo articula-se em particular com o Eixo 2 da ENSC, com o título “Prevenção, educação e sensibilização”.

Destacam-se os seguintes aspetos **positivos** nos dados apresentados, considerando os propósitos da ENSC:

- Os cuidados nas partilhas de dados pessoais *online*, o aumento das ações de sensibilização nas organizações e a diversidade de temáticas usadas nas ações de sensibilização a públicos externos contribuem para a concretização de diversas linhas de ação ligadas a atitudes, comportamentos e sensibilização face à cibersegurança;
- O aumento do número de cursos superiores de cibersegurança e segurança da informação, bem como de alunos inscritos e diplomados, também contribui para que algumas linhas de ação se realizem, sobretudo as relativas à educação.

Aspetos **negativos** que exigem consideração no desenvolvimento de uma nova ENSC:

- A elevada exposição ao risco *online*, a falta de alcance das ações de sensibilização para a cibersegurança e a carência de avaliação dos resultados das ações realizadas são desafios para as atitudes, comportamentos e sensibilização;
- A falta de competências em cibersegurança nas organizações é um problema, particularmente para o sistema educativo e de formação avançada.

Para mais detalhe quanto a esta articulação com linhas de ação específicas da ENSC, ver ANEXO.



O TERMO DE BUSCA
'BURLA *ONLINE*' VIU O SEU
ÍNDICE DE PESQUISAS A
CRESCER 80% E O TERMO
'OLÁ PAI, OLÁ MÃE' PASSOU
DE 0 PARA 1.8 NO ÍNDICE DE
PESQUISA DA GOOGLE



C. INTRODUÇÃO

O *Relatório Cibersegurança em Portugal – tema Sociedade 2024* é um documento que anualmente analisa as atitudes, os comportamentos, a sensibilização e a educação face à cibersegurança, focando-se, portanto, na componente social deste domínio. Este estudo sistematiza dados disponíveis sobre estas matérias, como os do Eurostat e da Direção-Geral de Estatísticas da Educação e Ciência (DGEEC), e recolhe outros através de fontes abertas ou de inquéritos à comunidade, como os relativos à sensibilização e educação. À parte a análise global feita anteriormente, o documento divide-se em quatro capítulos centrais:

- Exposição ao digital, no qual se analisa o volume de utilizações de serviços digitais críticos para a cibersegurança e, portanto, a exposição dos indivíduos e das organizações aos mesmos;
- Interesse pela “cibersegurança” nos *media* e nas pesquisas *online*, em que se acompanha a presença de termos ligados à cibersegurança nos meios de comunicação social e nas pesquisas realizadas *online*, de modo a compreender a saliência social do tema;
- Atitudes e comportamentos, em que se sistematizam dados que descrevem a sensibilização para a cibersegurança e as boas práticas aplicadas nas organizações e indivíduos;
- Sensibilização e educação, dedicado à apresentação de dados e tendências sobre as ações de sensibilização realizadas e a presença da cibersegurança no ensino superior.

Este documento faz ainda recomendações às organizações e indivíduos no sentido de mitigarem os riscos e vulnerabilidades associados a algumas das tendências identificadas. Para um melhor entendimento da metodologia utilizada, faculta-se uma nota metodológica no final.



D. EXPOSIÇÃO AO DIGITAL

O número de pessoas a utilizar a Internet e certos serviços digitais tem implicações no nível de exposição ao risco no ciberespaço. Para essa análise, de seguida, recorre-se a dados do Eurostat e da DGEEC.

O USO DA INTERNET

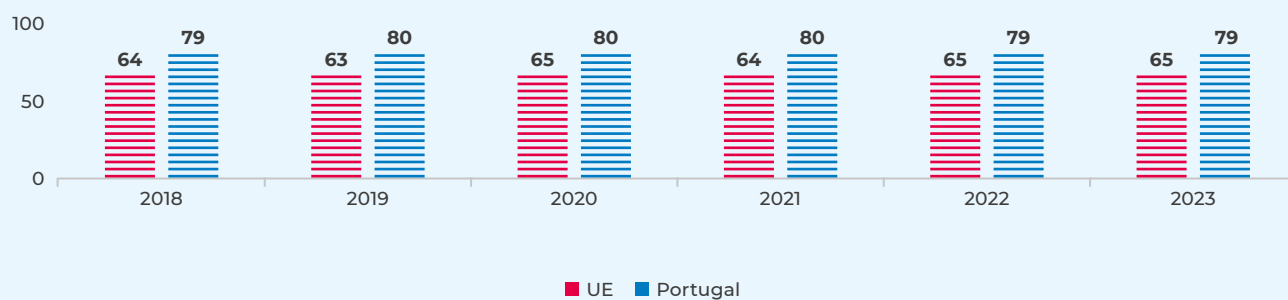
- O número de indivíduos a utilizar a Internet nos últimos 3 meses, em Portugal, aumentou 1 ponto percentual (pp), de 85% em 2022 para 86% em 2023 (o valor mais alto de sempre). Ainda assim, mantém-se abaixo da média da UE, a qual atinge os 91% (Eurostat, 2023a);
 - Quer nas empresas, quer na Administração Pública, a percentagem de organizações a usar banda larga mantém-se estável e muito elevada: 95% das Empresas (Eurostat, 2023b), 96% da Administração Pública Central e 100% das Câmaras Municipais (DGEEC, 2024).
-

USOS DE SERVIÇOS DIGITAIS CRÍTICOS PARA A CIBERSEGURANÇA

- Do ponto de vista das atividades realizadas *online* não existem grandes alterações em relação ao ano anterior, mantendo-se a existência de mais utilizadores em Portugal do que na média da UE a usar certas plataformas críticas para a cibersegurança nos últimos três meses: 88% dos indivíduos a usar *email* contra 86% na média da UE; 82% a telefonar ou usar chamadas de vídeos *online* contra 75% na média da UE; 79% a usar redes sociais para 65% na média da UE (ver figura 1); e 92% a usar mensagens instantâneas para 82% na média da UE (Eurostat, 2023c);

Figura 1

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



Fonte: Eurostat, 2023c

- Diferentemente, em Portugal usa-se menos o banco *online*, com 69% dos indivíduos, do que a média da UE, com 70% (Eurostat, 2023c); e 45% realizam compras *online*, para 58% na média da UE (Eurostat, 2023d).

E. INTERESSE PELA “CIBERSEGURANÇA” NOS MÉDIA E NAS PESQUISAS ONLINE

O nível de interesse pela cibersegurança por parte dos indivíduos e dos *mídia* permite compreender e comparar entre anos a importância desta temática numa sociedade. Para o efeito, de seguida analisa-se o número de artigos publicados nos *mídia* com a menção a “cibersegurança” e certas ciberameaças (através da plataforma Mediacloud)² e as pesquisas no motor de busca Google relacionadas com o tema (mediante o Google Trends)³.

NÚMERO DE ARTIGOS PUBLICADOS NOS MÉDIA QUE MENCIONARAM O TERMO “CIBERSEGURANÇA”

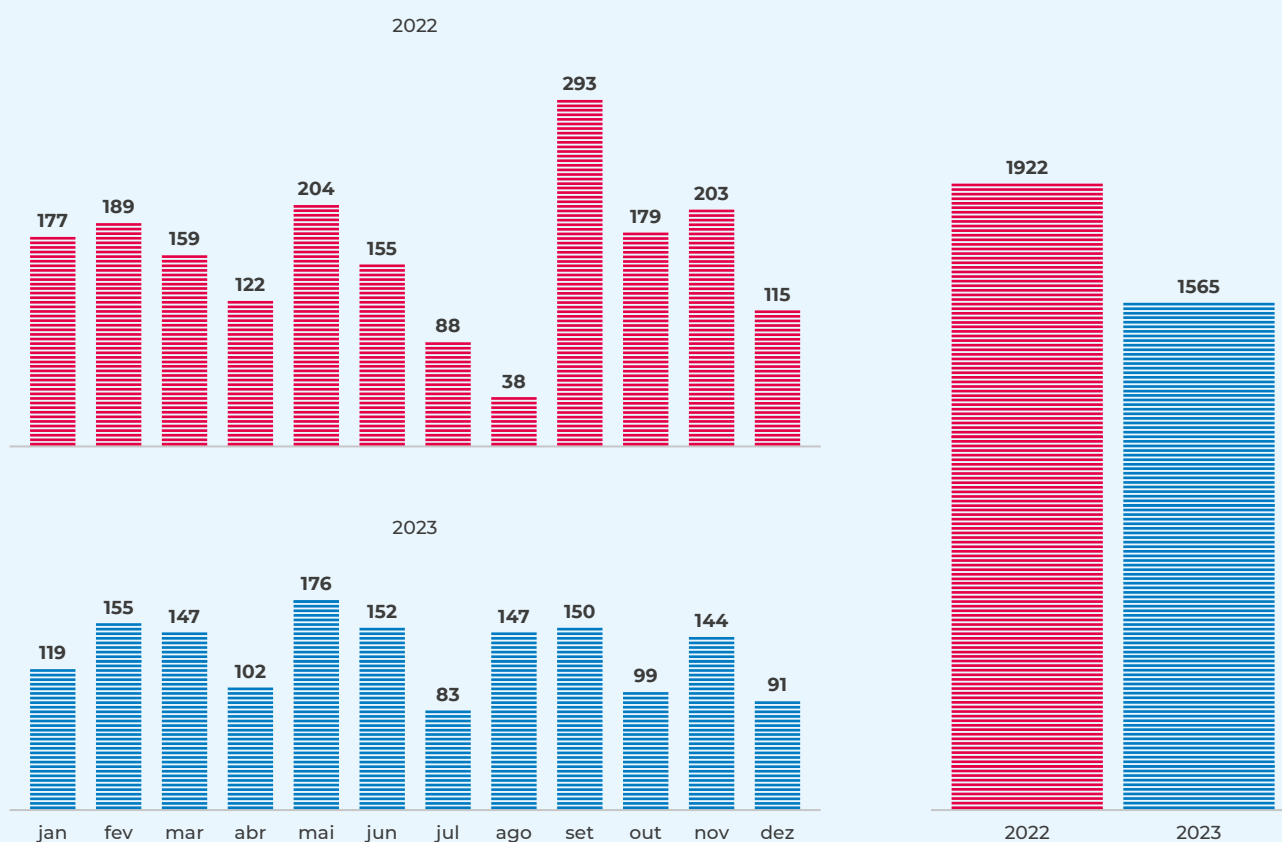
- Através da plataforma Mediacloud, é possível verificar o número de artigos publicados nos *mídia* que mencionaram o termo “cibersegurança” em Portugal. Comparando 2023 com 2022, verificou-se um decréscimo de 19% no número de artigos, os quais passaram de 1922 em 2022 para 1565 em 2023 (ver figura 2);
- Ao contrário de 2022, em que se verificaram várias flutuações na saliência do tópico ao longo do ano, em 2023 ocorre uma distribuição de atenção relativamente mais homogénea;
- Considerando os artigos dos *mídia* sobre ciberameaças em particular, nota-se que, embora o número de artigos sobre cibersegurança e sobre as ciberameaças mais típicas (como *ransomware*, *phishing* ou *burlas online*) tenham diminuído, encontramos mais artigos sobre *CEO Fraud* (passando de 19 artigos em 2022 para 38 em 2023) e sobre *spoofing* (passando de 6 para 21) (Mediacloud).

2. Ver nota metodológica para mais detalhes sobre a metodologia utilizada.

3. Ver nota metodológica para mais detalhes sobre a metodologia utilizada.

 Figura 2

NÚMERO DE ARTIGOS PUBLICADOS NOS MEDIA QUE MENCIONARAM O TERMO “CIBERSEGURANÇA” EM PORTUGAL



Fonte: Mediacloud

ÍNDICE DE PESQUISAS GOOGLE COM O TERMO “CIBERSEGURANÇA”

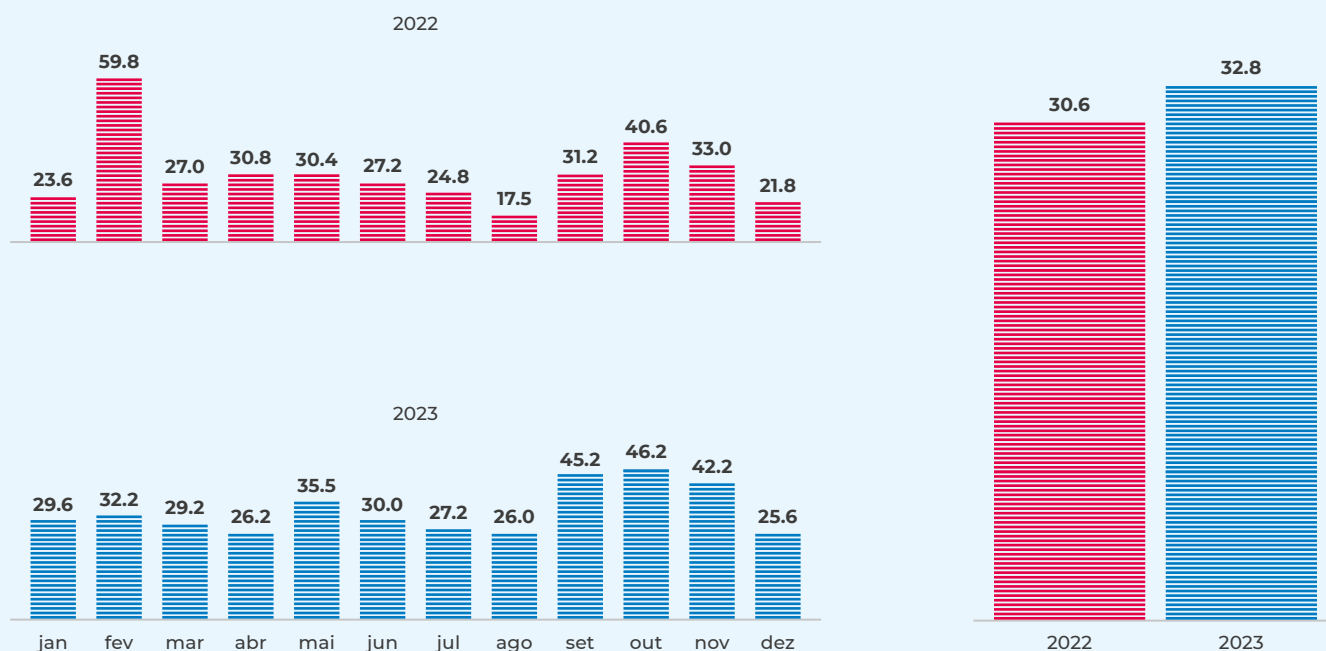
- Contrariamente ao observado no caso dos *media*, nota-se um maior interesse pela “cibersegurança” em 2023 nas pesquisas no motor de busca Google analisadas através da plataforma Google Trends. À luz do índice de popularidade relativa com base nas pesquisas realizadas⁴, verificou-se uma maior popularidade em 2023 (média de 32,8) do que em 2022 (média de 30,6). Ao contrário do que foi observado em 2022, em que o mês de fevereiro destaca-se claramente, em 2023 o interesse manteve-se relativamente homogêneo, sendo, contudo, mais elevado nos meses de setembro, outubro e novembro (ver figura 3);

4. “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 3

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

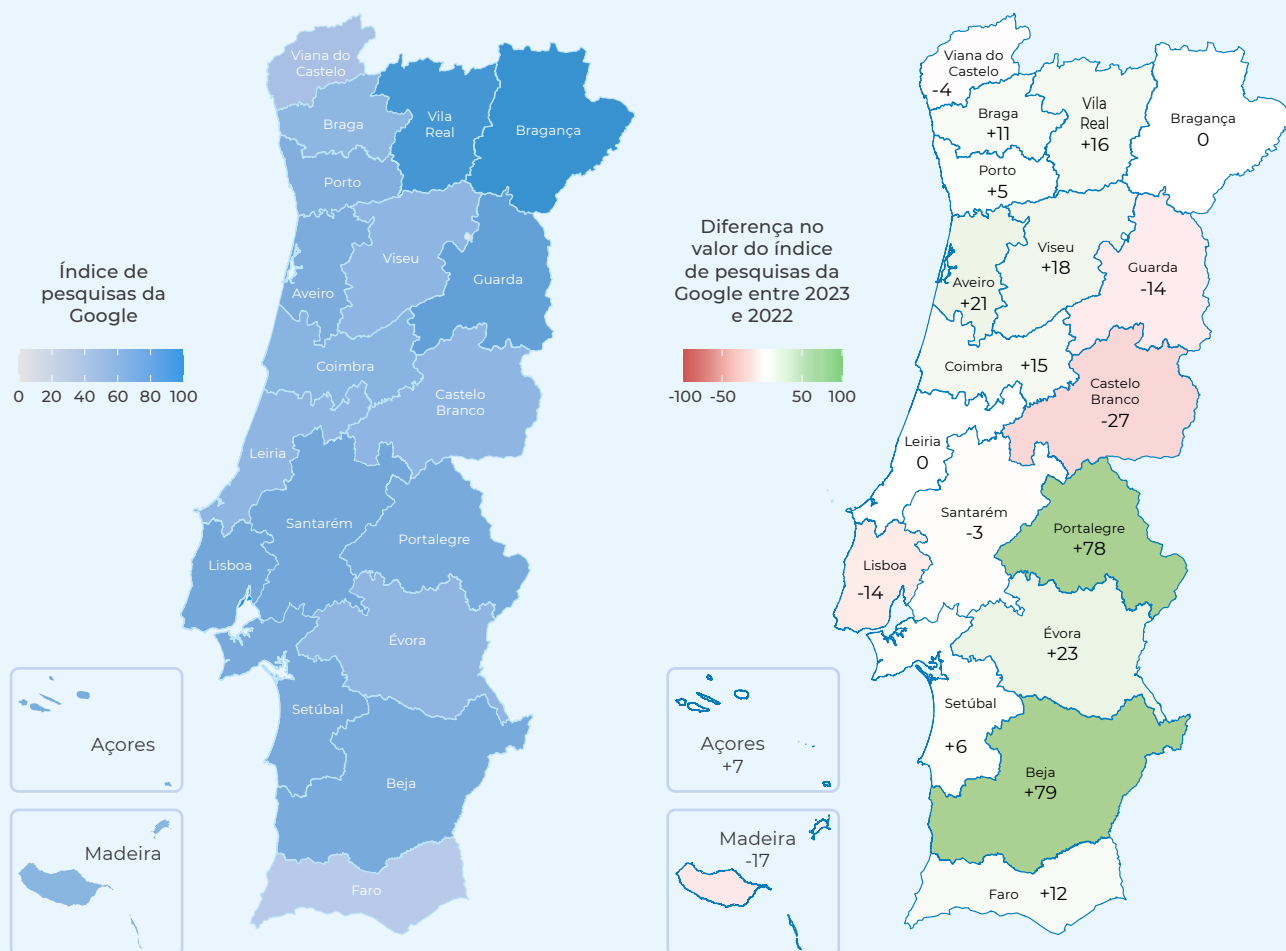


Fonte: Google Trends

- Relativamente às ciberameaças, o termo de busca “burla online” viu o seu índice de pesquisas a crescer 80% e o termo “olá pai, olá mãe” passou de 0 para 1.8 no índice de pesquisa da Google. Observou-se um grande decréscimo nos termos “ransomware” (na ordem dos 60%) e “malware” (11%);
- Do ponto de vista regional, verificou-se um valor mais elevado no índice de pesquisas da Google pela palavra “cibersegurança” em Bragança, Vila Real, Guarda e Lisboa do que nas restantes regiões em 2023. Foi na Madeira, Faro, Açores e Viana do Castelo onde se verificaram os valores mais baixos de pesquisas sobre este tema⁵ (ver figura 4);
- Comparativamente ao ano anterior, verificou-se um crescimento significativo em Beja e em Portalegre. Castelo Branco, Guarda, Madeira e Lisboa, pelo contrário, apresentam os maiores decréscimos relativamente ao ano transato (Google Trends).

5. 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).

ÍNDICE DE PESQUISAS GOOGLE COM O TERMO “CIBERSEGURANÇA” EM PORTUGAL, POR REGIÃO



Fonte: Google Trends



“ EM PORTUGAL, 80% DAS
EMPRESAS CONSIDERAM QUE
A CIBERSEGURANÇA É UMA
PRIORIDADE BASTANTE ALTA
OU MUITO ELEVADA ”

F. ATITUDES E COMPORTAMENTOS

As atitudes e os comportamentos remetem para a sensibilização para o tema e para as práticas efetivas correspondentes, quer nas pessoas, quer nas organizações. Esta análise será feita com o suporte de dados do Eurostat, do Eurobarómetro e da DGEEC.

COMPORTAMENTOS DOS INDIVÍDUOS

- Recorrendo de novo a dados do Eurostat, é possível concluir que, em Portugal, no ano de 2023, 46% dos indivíduos, nos últimos 3 meses, verificou se os *websites* a que os seus dados pessoais são fornecidos são seguros, o mesmo valor do último inquérito, em 2021. A média da UE foi de 32%;
- Em 2023, 72% dos indivíduos em Portugal aplicaram pelo menos uma das seis práticas de gestão dos dados na Internet elencadas no inquérito do Eurostat⁶, o mesmo que em 2021. A média da UE foi de 67%. A este respeito, em Portugal, os mais jovens (entre 16 e 24 anos) atingem os 93% (77% na UE) e os mais velhos (entre 65 e 74 anos) 35% (43% na UE) – portanto, a fratura digital é maior em Portugal do que na média da UE (Eurostat, 2023e).

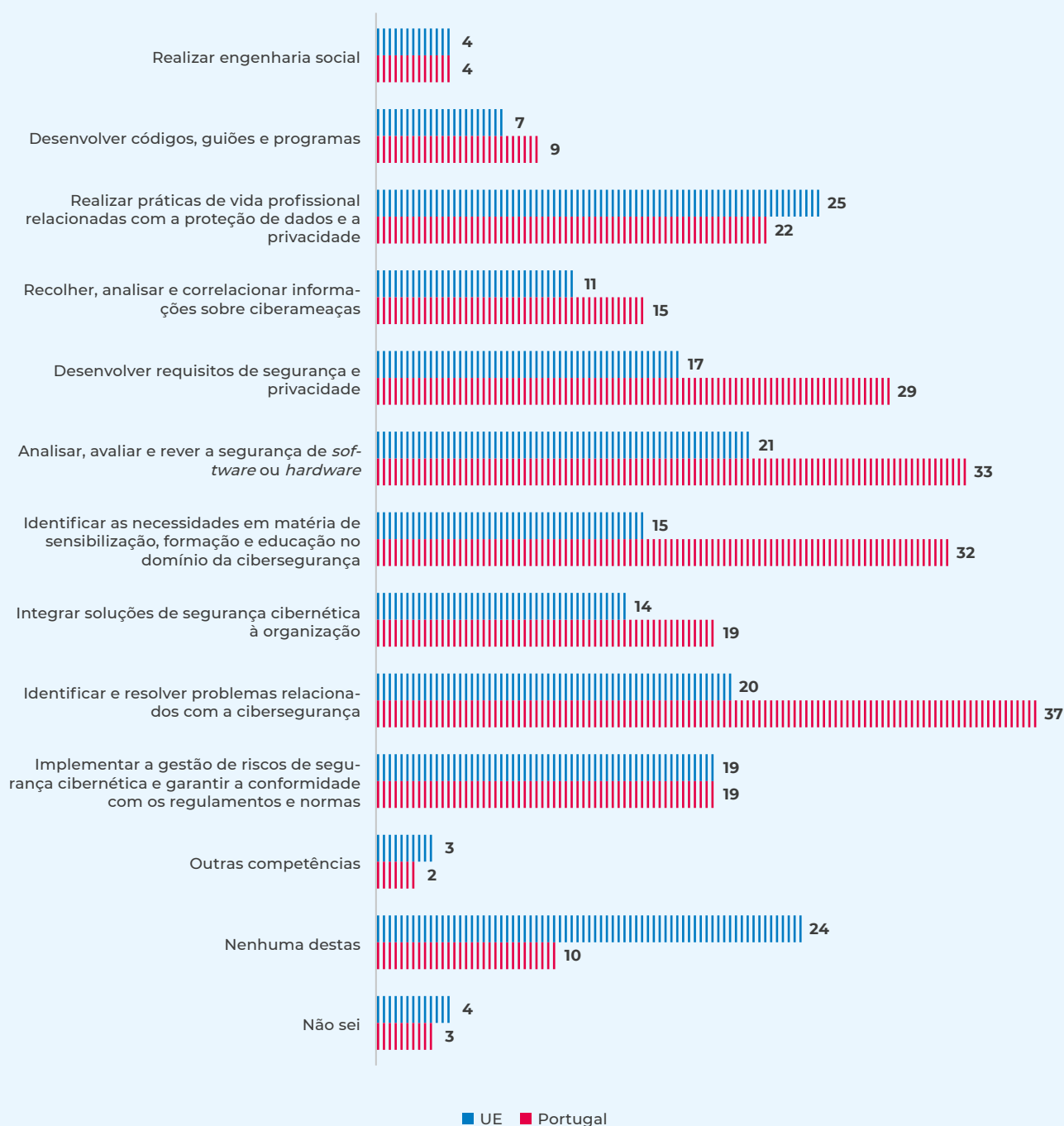
6. Ler as declarações de confidencialidade antes de fornecer dados pessoais; acesso restrito ou recusado à localização geográfica; acesso limitado a perfis ou conteúdos em sítios de redes sociais ou armazenamento em linha partilhado; recusa da utilização de dados pessoais para fins publicitários; verificar se o sítio *web* onde os dados pessoais fornecidos eram seguros; solicitar ao administrador ou fornecedor de sítios *web* ou motores de pesquisa que acedesse aos dados que detêm sobre si para os atualizar ou apagar.



COMPETÊNCIAS EM CIBERSEGURANÇA NAS EMPRESAS

- Com base em inquérito especial do Eurobarómetro (2024) sobre competências em cibersegurança nas empresas é possível concluir que, em 2024, em Portugal, 80% das empresas consideram que a cibersegurança é uma prioridade bastante alta ou muito elevada. Na média da UE o valor é de 71%;
- As empresas em Portugal recorrem mais a indivíduos ou empresas exteriores para tratarem de aspetos ligados à cibersegurança, atingindo os 60%, do que a média da UE, que fica pelos 51%;
- Cerca de 64% das empresas em Portugal têm pelo menos 1 funcionário a executar tarefas de cibersegurança, quando a média da UE é inferior, ficando pelos 57%;
- A maioria destes funcionários combina a cibersegurança com outras tarefas (59% em Portugal e 57% na média da UE) e foram recrutados para tarefas não relacionadas com a cibersegurança (40% em Portugal e 34% na média da UE);
- Em Portugal, 16% das empresas consideram que foi difícil encontrar e contratar pessoal com as competências adequadas em cibersegurança nos últimos 12 meses – a média da UE é de 12%. Os maiores obstáculos são a falta de candidatos (51% em Portugal e 44% na média da UE); a dificuldade em encontrar candidatos qualificados (40% em Portugal e 45% na média da UE); a falta de sensibilização para as funções de cibersegurança (37% em Portugal e 22% na média da UE); e os requisitos de credenciação de segurança (29% em Portugal e 16% na média da UE);
- Cerca de 77% das empresas inquiridas em Portugal afirmam não ter cargos em cibersegurança abertos a contratações, na média da UE este valor atinge os 87%; e 10% em Portugal têm uma posição aberta para esta área, enquanto a nível da UE a média é de 7%;
- As funções de cibersegurança consideradas mais importantes pelas empresas em Portugal são as de responsável principal pela segurança/informação (47% em Portugal e 30% na média UE); especialista em formação em matéria de segurança (39% em Portugal e 17% na média UE); e responsável pela resposta a incidentes (20% em Portugal e 16% na média da UE);
- As competências em cibersegurança consideradas mais relevantes pelas empresas em Portugal são as de identificar e resolver problemas relacionados com a cibersegurança (37% em Portugal e 20% na média da UE); analisar, avaliar e rever a segurança de *software* ou *hardware* (33% em Portugal e 21% na média da UE); e identificar as necessidades em matéria de sensibilização, formação e educação no domínio da cibersegurança (32% em Portugal e 15% na média da UE - ver figura 5) (Eurobarómetro, 2024).

COMPETÊNCIAS DE CIBERSEGURANÇA CONSIDERADAS MAIS IMPORTANTES NA EMPRESA, 2024 (%)



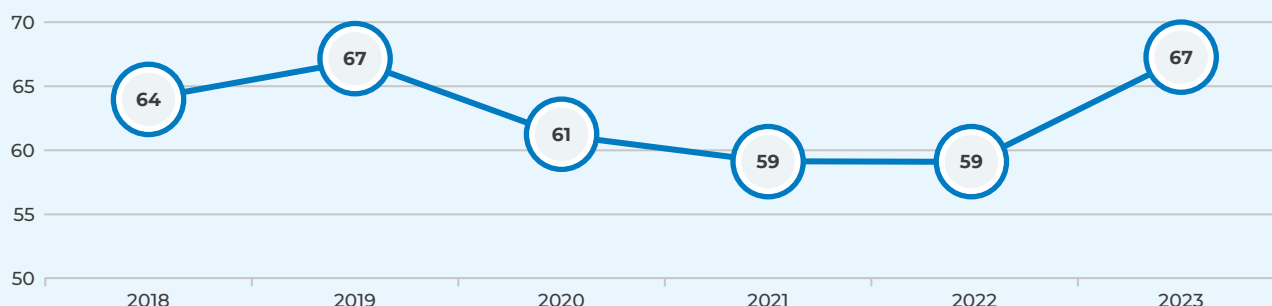
Fonte: Eurobarómetro, 2024

CIBERSEGURANÇA NA ADMINISTRAÇÃO PÚBLICA

- Com base nos dados dos dois Inquéritos sobre a Utilização das Tecnologias de Informação e Comunicação (TIC) na Administração Pública Central e Regional, bem como nas Câmaras Municipais, da DGEEC, produzidos anualmente, é possível acompanhar a situação do setor público no domínio da cibersegurança. A este respeito, a percentagem de organismos da Administração Pública com uma estratégia para a segurança da informação definida aumentou de 59% em 2022 para 67% em 2023, retomando o valor de 2019, depois de um contínuo decréscimo (ver figura 6). Nas Câmaras Municipais é onde este aumento foi mais acentuado, de 60% para 71%;

 Figura 6

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



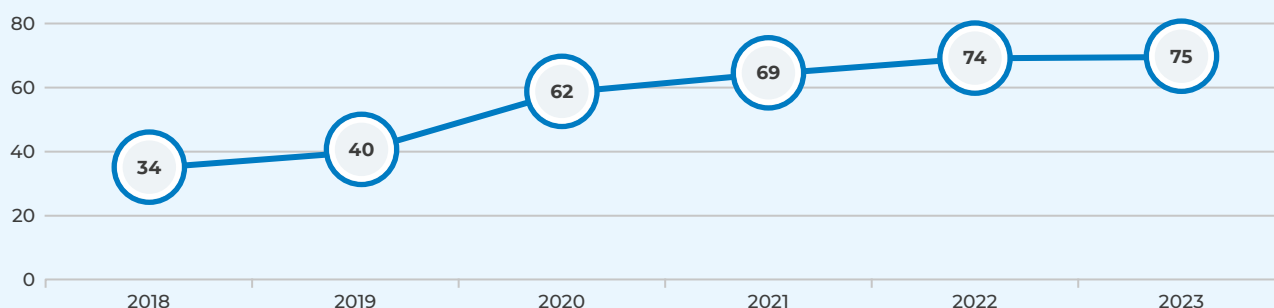
Fonte: DGEEC 2019-2024

- Verifica-se um decréscimo significativo no uso de MFA por parte dos organismos públicos, de 71% em 2022 para 49% em 2023, uma descida de 22 pp;
- Por sua vez, há um aumento significativo de entidades a ter um inventário de ativos essenciais para a prestação dos serviços de segurança das TIC entre 2022 e 2023, de 63% para 82%, respetivamente; a ter controlo de acessos remotos, de 76% para 93%; e a conservar os logs, de 67% para 80%;

- A percentagem de organismos da Administração Pública que afirmam ter necessidade elevada de reforço de competências em segurança das TIC continua a aumentar, tendo passado de 74% em 2022 para 75% em 2023 (ver figura 7). Na Administração Pública Central há uma redução de 70% para 69%, mas nas Câmaras Municipais há um aumento de 86% para 89%⁷;

 Figura 7

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 2019-2024

- Verifica-se um aumento no número de organismos da Administração Pública a recorrer a um misto de pessoal próprio e fornecedores externos na realização de atividades relacionadas com a segurança das TIC, de 19% em 2022 para 49% em 2023, passando a representar a maioria do tipo de pessoal alocado. Em 2023 e anos anteriores dominava o pessoal do próprio organismo apenas alocado a estas atividades;
- A percentagem de organismos da Administração Pública com recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC aumentou de 46% em 2022 para 52% em 2023 (DGEEC, 2024a e 2024b).

7. Ao contrário de anos anteriores, não parece existir correlações positivas ou negativas entre a definição de Estratégias para a Segurança da Informação e a elevada necessidade de competências em segurança das TIC nas Câmaras Municipais.



EM 2024 EXISTEM 37 CURSOS
SUPERIORES DE CIBERSEGURANÇA
E SEGURANÇA DA INFORMAÇÃO
EM PORTUGAL, MAIS 8 DO QUE NO
ANO ANTERIOR



G. SENSIBILIZAÇÃO E EDUCAÇÃO

O domínio da sensibilização e da educação neste relatório traz visibilidade sobre o que se realiza em termos de capacitação humana em cibersegurança. Enquanto a sensibilização procura promover as competências mais básicas e transversais, a educação aprofunda as especializadas e técnicas. Para a análise destas componentes, realizou-se um inquérito e recolheram-se dados de fontes abertas, nomeadamente da Direção-Geral de Ensino Superior (DGES) e da DGEEC. Consideram-se ainda dados do Eurobarómetro e do Eurostat.

AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA

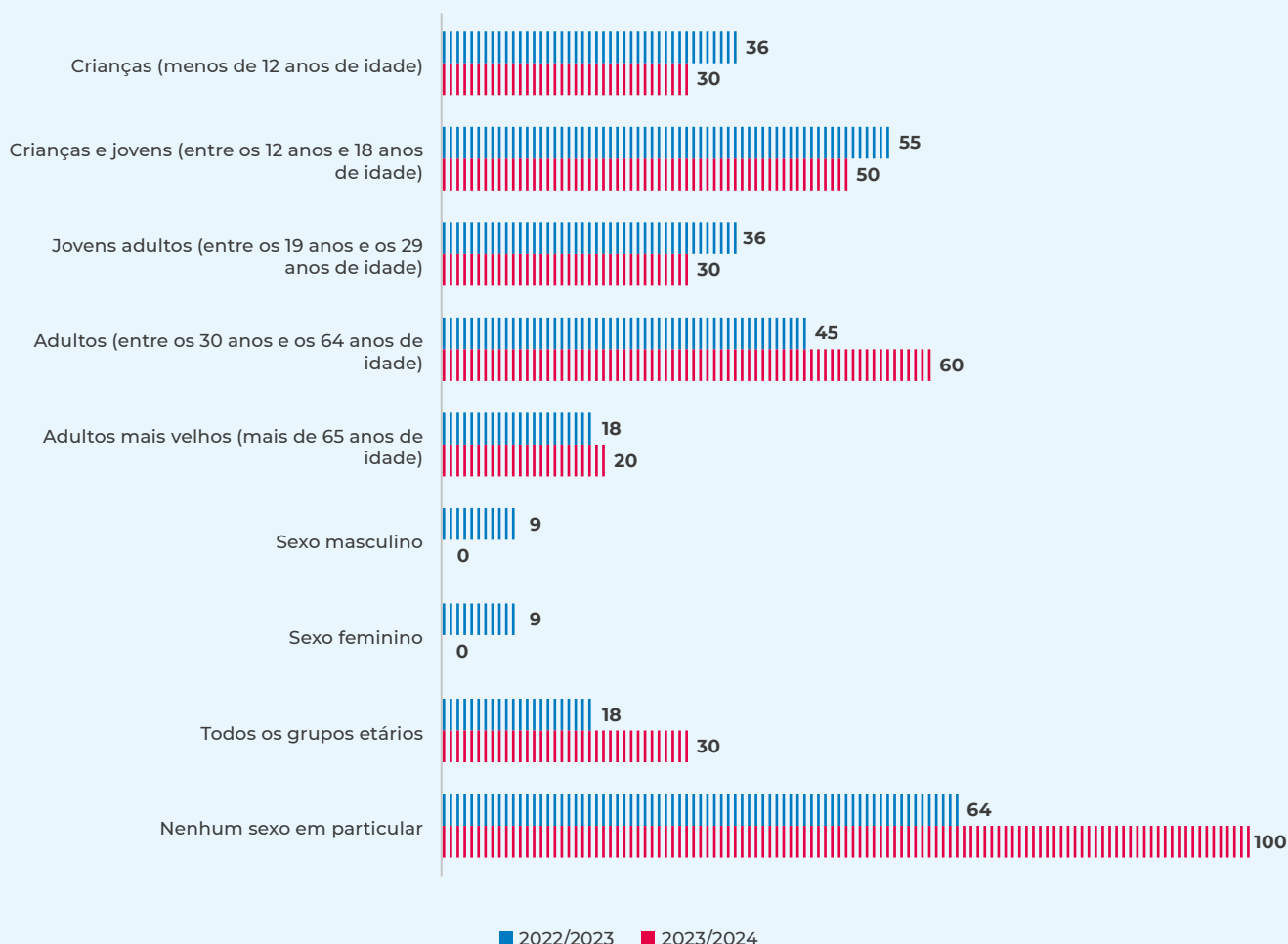
- Com base em inquérito anual realizado em Portugal pelo Observatório de Cibersegurança a entidades selecionadas que realizam ações de sensibilização em cibersegurança destinadas a públicos externos, sem fins lucrativos, conclui-se que em 2023 ocorreram pelo menos 1283 ações deste tipo⁸;
- Estima-se que estas ações alcançaram cerca de 300 mil pessoas no âmbito de sessões presenciais e à distância, bem como cursos *online*, e cerca de 5 milhões e meio de visualizações nas redes sociais e visitas a *websites*;
- Entre as ações de sensibilização realizadas, 69% foram sessões presenciais ou à distância; 25%, cursos *online*; 3%, campanhas nas redes sociais; 3%, outros; e 1%, campanhas na comunicação social;
- Verifica-se uma tendência para um incremento de adultos como público-alvo das ações de sensibilização realizadas entre 2023 e o primeiro semestre de 2024, estando presente nas estratégias de 60% das entidades que responderam ao inquérito. As crianças e jovens são o segundo grupo etário mais visado, com 50% (ver figura 8). Ao contrário de anos anteriores, nenhuma entidade destacou um dos sexos como público-alvo predominante;

8. Inquérito que abrangeu todas as entidades envolvidas no Centro Internet Segura (49 entidades, incluindo o CNCS), juntamente com APDSI, AP2SI, CIIWA, COTEC e IAPMEI (os valores apresentados sobre público alcançado são estimativos).



Figura 8

CARACTERIZAÇÃO ETÁRIA E POR SEXO DO PÚBLICO-ALVO PREDOMINANTE VISADO PELAS ENTIDADES SELECIONADAS QUE REALIZAM AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA (ESTIMATIVA), EM PORTUGAL (%)*

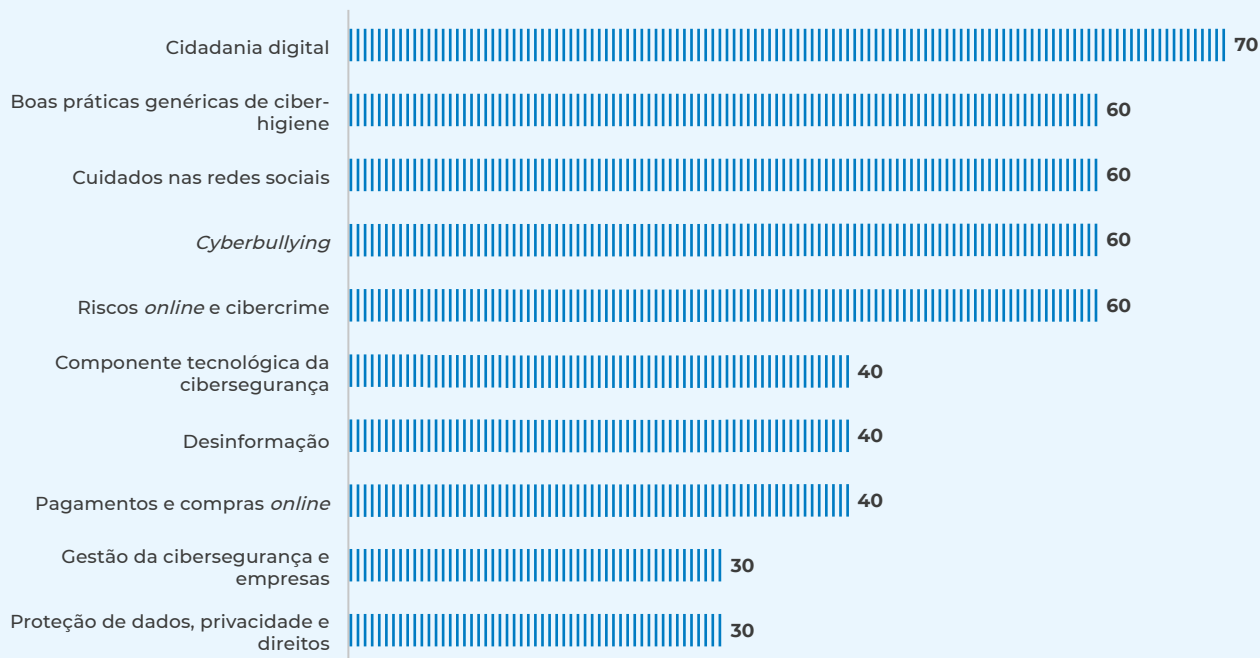


*Múltiplas respostas possíveis. Os valores referentes a 2024 compreendem apenas o 1º semestre.

Fonte: CNCS

- Os temas mais tratados nas ações de sensibilização realizadas entre 2023 e o primeiro semestre de 2024 foram Cidadania digital, Boas práticas genéricas de ciber-higiene, Cuidados nas redes sociais, Cyberbullying e Riscos online e cibercrime (ver figura 9);

TEMAS TRATADOS NAS AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA REALIZADAS EM PORTUGAL, POR ENTIDADES COM ESSA MISSÃO SELECIONADAS, EM 2023/2024 (%) - TOP 10 *



*Múltiplas respostas possíveis. Os valores referentes a 2024 compreendem apenas o 1º semestre.

Fonte: CNCS

- Tal como em anos anteriores, a percentagem de entidades a avaliar o impacto das suas ações de sensibilização nos comportamentos do público-alvo é reduzida. Apenas 30% das entidades inquiridas afirmam fazê-lo, sendo que os métodos mais utilizados são as análises estatísticas de organismos de referência (para dois terços), seguida dos inquéritos e da observação direta, ambos com um terço cada (inquérito CNCS).

SENSIBILIZAÇÃO NAS EMPRESAS E NA ADMINISTRAÇÃO PÚBLICA

- Apenas 26% das empresas em Portugal haviam fornecido formação ou sensibilização sobre cibersegurança nos últimos 12 meses aos seus funcionários, no momento do inquérito do Eurobarómetro já mencionado – a média da UE é de 25% (Eurobarómetro, 2024);
- A percentagem de organismos da Administração Pública a realizar ações de sensibilização aumentou em todas as tipologias: voluntárias (de 69% em 2022 para 75% em 2023); obrigatórias (de 24% para 32%); e em disposições contratuais (de 28% para 30%) (DGEEC, 2024a e 2024b).

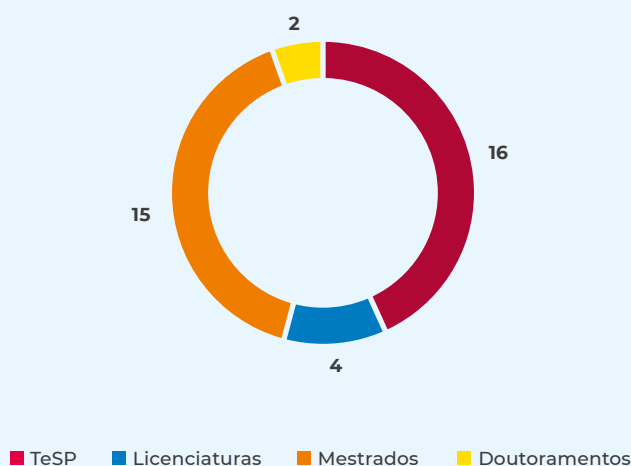
CURSOS DO ENSINO SUPERIOR EM CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

- De acordo com dados da DGES, em 2024 existem 37 cursos superiores de cibersegurança e segurança da informação em Portugal, mais 8 do que no ano anterior⁹. São 16 Cursos Técnicos Superiores Profissionais (TeSP), 15 mestrados, quatro licenciaturas e dois doutoramentos (ver figura 10).



Figura 10

TOTAL DE CURSOS SUPERIORES DE CIBERSEGURANÇA E SEGURANÇA DE INFORMAÇÃO EM PORTUGAL, POR TIPO/GRAU, 2024



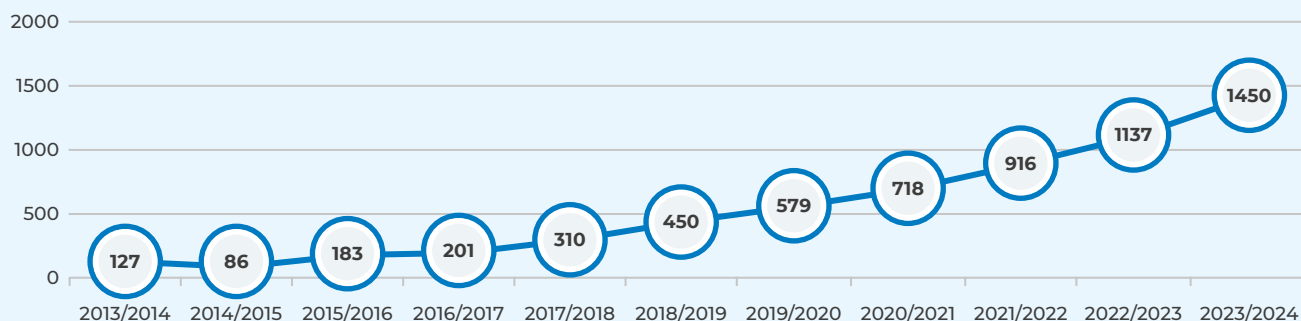
Fonte: DGES (recolha CNCS)

- Cerca de 43% destes cursos encontram-se no Norte do país, 35% na Área Metropolitana de Lisboa, 16% no Centro e 5% no Alentejo. A maioria dos cursos são públicos (70%) (DGES – recolha CNCS);
- O número de alunos inscritos em cursos superiores de cibersegurança e segurança da informação continua a aumentar, passando de 1137 em 2022/2023 para 1450 em 2023/2024, crescendo 28% (ver figura 11) - a percentagem de mulheres inscritas em 2023/2024 foi 9%, menos 1 pp do que no ano anterior (DGEEC – recolha CNCS);

9. Por equívoco faltou somar um curso já existente no ano de 2023 no Relatório do ano passado (CNCS, 2023).


 Figura 11

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

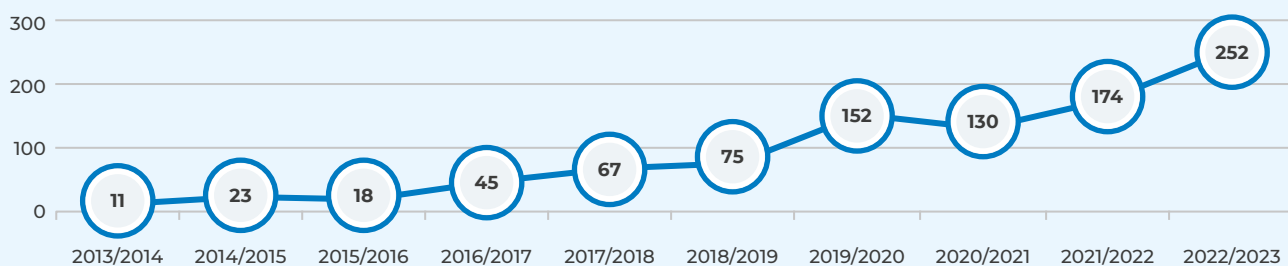


Fonte: DGEEC (recolha CNCS)

- O número de diplomados em 2022/2023 aumentou 45%, de 174 para 252; a percentagem de mulheres aumentou 1 pp, de 7% para 8% no mesmo período (ver figura 12) (DGEEC – recolha CNCS). Este valor mantém-se bastante abaixo da percentagem de mulheres diplomadas em cursos superiores de TIC, que em 2023 atingiu os 21,8%, mais 1,3 pp do que ano anterior (Pordata)¹⁰.


 Figura 12

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



Fonte: DGEEC (recolha CNCS)

10. <https://prod2.pordata.pt/db/portugal/ambiente+de+consulta/tabela> [consultado a 19/11/2024]

H. RECOMENDAÇÕES

Apresenta-se no quadro seguinte algumas recomendações considerando os aspetos mais críticos identificados no presente documento:



Quadro 2

Aspetos críticos	Recomendações
Elevada exposição ao risco em resultado de existirem muitos utilizadores de certos serviços digitais críticos para a cibersegurança	Continuar a promover ações de sensibilização, formação e educação em matéria de cibersegurança junto dos cidadãos em geral, tendo em conta as especificidades de cada população, com avaliação de necessidades e do impacto das ações
Dificuldades das organizações em contratar e especializar profissionais de cibersegurança	Formar e requalificar profissionais na área da cibersegurança, quer através de cursos de ensino superior, quer de programas de formação avançada
Aplicação insuficiente de algumas medidas nas organizações, nomeadamente o MFA	Promover junto das organizações públicas e privadas as 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, focando em particular a aplicação do MFA
Falta de potencial de alcance das ações de sensibilização dirigidas ao público em geral	Investir em meios de comunicação com mais alcance nas ações de sensibilização para a cibersegurança realizadas
Carência de avaliação dos resultados nos comportamentos do público-alvo das ações de sensibilização realizadas	Avaliar junto dos públicos-alvo as ações de sensibilização para a cibersegurança realizadas, sobretudo no que diz respeito a mudanças positivas de comportamento, através, por exemplo, de inquéritos, entrevistas e testes de engenharia social

Recursos de capacitação do CNCS: 4 MOOCs (Cidadão Ciberseguro, Cidadão Ciberinformado, Consumidor Ciberseguro e Cidadão Ciber social), 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 METODOLÓGICAS

O presente documento é realizado através da sistematização de três tipos de dados: estatísticas disponibilizadas por entidades especializadas na sua produção, como o Eurostat e a DGEEC; informação organizada pelo CNCS e recolhida em fontes abertas, como as da DGES e parte dos dados da própria DGEEC; e valores produzidos diretamente pelo CNCS através de inquérito, como é o caso da dimensão ligada às ações de sensibilização.

Estes dados são analisados de forma integrada, tendo em conta as temáticas deste relatório, de modo a proporcionar um diagnóstico nacional sobre a componente social da cibersegurança. Esta visão panorâmica apresenta-se na Análise Global.

Os números sobre o uso da Internet e de serviços digitais críticos, bem como os relativos à privacidade e proteção dos dados pessoais, foram desenvolvidos pelo Eurostat (Eurostat, 2023a; 2023c; 2023d). O Instituto Nacional de Estatística é o responsável pela sua recolha em Portugal. Estes dados foram produzidos através do inquérito *ICT usage in households and by individuals*, dirigido a contextos domésticos com Internet, nos quais pelo menos uma pessoa tenha entre 16 e 74 anos. Foi realizado entre 4 de maio e 31 de julho de 2023 em Portugal, tendo sido entrevistadas 7672 pessoas. Para mais detalhe consultar a seguinte página:

→ https://ec.europa.eu/eurostat/cache/metadata/EN/isoc_i_simsih2_pt.htm

No que se refere ao uso da Internet nas empresas (Eurostat 2023b), os valores são recolhidos pelas mesmas entidades referidas, mas mediante o inquérito *ICT usage in enterprises*, entre 15 de fevereiro e 31 de julho de 2023 em Portugal, tendo sido dirigido a 9510 empresas. Para mais detalhe consultar seguinte página:

→ https://ec.europa.eu/eurostat/cache/metadata/EN/isoc_e_simsie_pt.htm

A análise sobre o interesse pela “cibersegurança” nos *media* e nas pesquisas *online* em Portugal efetuou-se com recurso à plataforma Mediacloud, para recolha e análise do número de artigos publicados nos *media*, e à plataforma Google Trends, no que diz respeito às pesquisas *online*. Para a recolha dos dados na plataforma Mediacloud foram utilizados 89 meios de comunicação. Para mais detalhe relativamente a Google Trends e Mediacloud, consultar as seguintes páginas:

→ www.mediacloud.org/documentation/search-tool-guide

→ <https://trends.google.pt/trends/>



A componente referente às competências em cibersegurança foi desenvolvida a partir do inquérito do Eurobarómetro feito no âmbito do *Flash Eurobarometer 547 Cyberskills*, o qual foi aplicado entre abril e maio de 2024, tendo sido conduzidas nesse período 503 entrevistas a empresas em Portugal. Para mais detalhe, consultar a seguinte página:

→ <https://europa.eu/eurobarometer/surveys/detail/3176>

Os dados sobre a Administração Pública são recolhidos anualmente pela DGEEC nos dois Inquéritos à Utilização das TIC - um dirigido à Administração Pública Central e Regional e o outro às Câmaras Municipais (DGEEC 2024a 2024b) - realizados entre setembro de 2023 e fevereiro de 2024, obtendo-se as respostas de 384 organismos da Administração Pública Central e Regional e de 308 Câmaras Municipais. Para mais detalhes, consultar a seguinte página:

→ <https://www.dgeec.medu.pt/p/ciencia-e-tecnologia>

A informação apresentada sobre as ações de sensibilização foi recolhida no âmbito do inquérito sobre a Sensibilização para a Cibersegurança 2023/2024, realizado pelo Observatório de Cibersegurança do CNCS, dirigido às entidades que constituem o Centro Internet Segura e outras organizações consideradas relevantes no panorama das organizações que realizam ações de sensibilização em cibersegurança dirigidas a públicos externos ou educativos, num total de 54 organizações. O inquérito foi realizado entre os dias 4 e 18 de outubro de 2024 e responderam onze entidades.

A informação apresentada sobre o número de cursos de cibersegurança e segurança da informação, bem como alunos inscritos e diplomados nos mesmos, foi recolhida no *website* da DGES, no motor de pesquisa de cursos, utilizando-se para o efeito as palavras-chave “cibersegurança” e “segurança”. Relativamente ao número de alunos inscritos e diplomados, a informação foi recolhida no *website* da DGEEC, utilizando-se as mesmas palavras-chave. Para mais detalhe, consultar as seguintes páginas:

→ https://www.dges.gov.pt/simges/public/www/cursos_instituicoes?plid=372

→ <https://www.dgeec.medu.pt/p/ensino-superior> [*links* consultados a 19/11/2024]

Para esclarecimento de dúvidas adicionais sobre as metodologias adotadas, contactar o CNCS através do seguinte email: cnscs@cnscs.gov.pt

J. ENTIDADES PARCEIRAS NA REALIZAÇÃO DO RELATÓRIO

- **AP2SI** - Associação Portuguesa para a Promoção da Segurança da Informação
- **APAV** - Associação Portuguesa de Apoio à Vítima - Linha Internet Segura
- **APDSI** - Associação para a Promoção e Desenvolvimento da Sociedade da Informação
- **Associação DNS.PT** (.PT)
- **CIWA** - Competitive Intelligence & Information Warfare Association
- **Comissão Nacional de Promoção dos Direitos e Proteção das Crianças e Jovens**
- **COTEC Portugal** - Associação Empresarial para a Inovação
- **DECO** - Associação Portuguesa para a Defesa do Consumidor
- **DGE** - Direção-Geral da Educação (Centro de Sensibilização SeguraNet)
- **DGEEC** - Direção-Geral de Estatísticas da Educação e Ciência
- **IAPMEI** - Agência para a Competitividade e Inovação, I.P.
- **IPDJ** - Instituto Português do Desporto e Juventude, I.P.

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



K. 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)

CEO Fraud/Comprometimento de Email de CEO/Negócio: “A fraude de CEO/negócio acontece quando um funcionário de uma empresa [ou organização] é enganado de modo a pagar uma fatura falsa ou a fazer uma transferência não autorizada com a conta da empresa [ou organização].”

(Europol, Cyberscams)

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)

Spoofing: “falsificar o endereço de envio de uma comunicação para obter o acesso ilegal a um sistema”.

(NIST, IR 7298 Revision 2, Glossary of Key Information Security Terms)

- **AP2SI:** Associação Portuguesa para a Promoção da Segurança da Informação.
- **APDSI:** Associação para a Promoção e Desenvolvimento da Sociedade da Informação;
- **CNCS:** Centro Nacional de Cibersegurança.
- **COTEC [Portugal]:** Associação Empresarial para a Inovação.
- **DGEEC:** Direção-Geral de Estatísticas da Educação e Ciência.
- **DGES:** Direção-Geral de Ensino Superior.
- **ENSC:** Estratégia Nacional de Segurança do Ciberespaço 2019-2023.
- **IAPMEI:** Agência para a Competitividade e Inovação, I.P.
- **MOOC:** Curso Online Aberto e Massivo [Massive Open Online Course].
- **MFA:** Múltiplo Fator de Autenticação.
- **PME:** Pequenas e Médias Empresas.
- **pp:** pontos percentuais.
- **TeSP:** [Curso] Técnico Superior Profissional.
- **TIC:** Tecnologias de Informação e Comunicação.
- **UE:** União Europeia.

L. REFERÊNCIAS PRINCIPAIS

RELATÓRIOS

[consultados a 19/11/2024]:

- CNCS (2024) *Relatório Cibersegurança em Portugal – Riscos & Conflitos 2024*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em:
<https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obciber-cnccs.pdf>
- CNCS (2023) *Relatório Cibersegurança em Portugal – Sociedade de 2023*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em:
<https://www.cncs.gov.pt/docs/rel-sociedade2023-observ-cnccs-dig.pdf>
- CNCS (2019) *Relatório Cibersegurança em Portugal – Sociedade de 2019*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em:
<https://www.cncs.gov.pt/docs/relatorio-sociedade-2019-observatorio-de-cibersegurana-cnccs-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 19/11/2024]:

- DGEEC (2024a) *Inquérito à Utilização das Tecnologias da Informação e Comunicação na Administração Pública Central e Regional – IUTICAP 2023*. Direção-Geral de Estatísticas da Educação e Ciência. Disponível em:
<https://www.dgeec.mec.pt/np4/12.html>
- DGEEC (2024b) *Inquérito à Utilização das Tecnologias da Informação e Comunicação nas Câmaras Municipais- IUTICCM 2023*. Direção-Geral de Estatísticas da Educação e Ciência. Disponível em:
<https://www.dgeec.mec.pt/np4/12.html>

- Eurostat (2023a) *Individuals - internet use*. Eurostat Disponível em:
https://ec.europa.eu/eurostat/databrowser/view/ISOC_CI_IFP_IU__custom_12643419/default/table?lang=en
- Eurostat (2023b) *Type of connections to the internet by size class of enterprise*. Eurostat. Disponível em:
https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_it_es__custom_12643862/default/table?lang=en
- Eurostat (2023c) *Individuals – internet activities*. Eurostat. Disponível em:
https://ec.europa.eu/eurostat/databrowser/view/ISOC_CI_AC_I__custom_12643505/default/table?lang=en
- Eurostat (2023d) *Internet purchases by individuals (2020 onwards)*. Eurostat. Disponível em:
https://ec.europa.eu/eurostat/databrowser/view/ISOC_EC_IB20__custom_12643773/default/table?lang=en&page=time:2021
- Eurostat (2023e) *Privacy and protection of personal data (2020 onwards)*. Eurostat: Disponível em:
https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_prv20__custom_10133646/bookmark/table?lang=en&bookmarkId=7b1c4a8a-d308-46d5-97e4-4f41aab75ca8
- Eurobarómetro (2024) *Flash Eurobarometer 547 Cyberskills*. European Commission. Disponível em:
<https://europa.eu/eurobarometer/surveys/detail/3176>

OUTROS DOCUMENTOS

[consultados a 19/11/2024]:

- 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>
- Europol (2018) *Cybercams*. Europol EC3. Disponível em:
https://www.europol.europa.eu/sites/default/files/documents/pt_0.pdf
- 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>
- ISO/IEC 27032 (2012) *Information technology – Security techniques – Guidelines for cybersecurity*. International Standards Organization. Disponível em:
<https://www.iso.org/standard/44375.html>
- NIST (2013) *NIST IR 7298 Revision 2, Glossary of Key Information Security Terms*. National Institute of Standards and Technology. Disponível em:
<https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>



LEGISLAÇÃO E POLÍTICAS PÚBLICAS

(consultadas a 19/11/2024)

- 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 19/11/2024]:

- trends.google.com/trends/?geo=PT
- www.cncs.gov.pt
- www.dgeec.mec.pt
- <http://www.dges.gov.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 - <i>Prevenção, educação e sensibilização articuláveis com os indicadores deste relatório</i>		Área	Tendências positivas	Tendências negativas
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 – IN-CoDe.2030».	Sensibilização	Tendência positiva nos cuidados nas partilhas de dados pessoais <i>online</i> , na sensibilização nas organizações e nas temáticas usadas nas ações de sensibilização	Elevada exposição ao risco <i>online</i> , falta de alcance das ações de sensibilização para a cibersegurança e carência de avaliação dos resultados das ações realizadas
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.	Sensibilização	Tendência positiva nos cuidados nas partilhas de dados pessoais <i>online</i> , na sensibilização nas organizações e nas temáticas usadas nas ações de sensibilização	Elevada exposição ao risco <i>online</i> , falta de alcance das ações de sensibilização para a cibersegurança e carência de avaliação dos resultados das ações realizadas
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.	Atitudes, comportamentos e sensibilização	Tendência positiva nos cuidados nas partilhas de dados pessoais <i>online</i> , na sensibilização nas organizações e nas temáticas usadas nas ações de sensibilização	Elevada exposição ao risco <i>online</i> , falta de alcance das ações de sensibilização para a cibersegurança e carência de avaliação dos resultados das ações realizadas
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.	Educação	Aumento do número de cursos superiores de cibersegurança e segurança da informação, bem como de alunos inscritos e diplomados	Falta de competências em cibersegurança nas organizações
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.	Sensibilização	Tendência positiva nos cuidados nas partilhas de dados pessoais <i>online</i> , na sensibilização nas organizações e nas temáticas usadas nas ações de sensibilização	Elevada exposição ao risco <i>online</i> , falta de alcance das ações de sensibilização para a cibersegurança e carência de avaliação dos resultados das ações realizadas
E2k)	Valorizar a inclusão do comportamento consciente e responsável da utilização da tecnologia enquanto parte integrante e transversal da formação académica e profissional corrente.	Educação	Aumento do número de cursos superiores de cibersegurança e segurança da informação, bem como de alunos inscritos e diplomados	Falta de competências em cibersegurança nas organizações



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.	Sensibilização	Tendência positiva nos cuidados nas partilhas de dados pessoais <i>online</i> , na sensibilização nas organizações e nas temáticas usadas nas ações de sensibilização	Elevada exposição ao risco <i>online</i> , falta de alcance das ações de sensibilização para a cibersegurança e carência de avaliação dos resultados das ações realizadas
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.	Educação	Aumento do número de cursos superiores de cibersegurança e segurança da informação, bem como de alunos inscritos e diplomados	Falta de competências em cibersegurança nas organizações
E2r)	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.	Atitudes, comportamentos e sensibilização	Tendência positiva nos cuidados nas partilhas de dados pessoais <i>online</i> , na sensibilização nas organizações e nas temáticas usadas nas ações de sensibilização	Elevada exposição ao risco <i>online</i> , falta de alcance das ações de sensibilização para a cibersegurança e carência de avaliação dos resultados das ações realizadas

* Codificação atribuída com base no eixo em questão e na sequência pela qual surgem as linhas de ação, alinhadas com a ordem alfabética.



