CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

RELATÓRIO

CIBERSEGURANÇA EM PORTUGAL

SOCIEDADE 2021

3ª EDIÇÃO

DEZEMBRO DE 2021

Observatório
de **Cibersegurança**

ÍNDICE

03 **A. Sumário executivo**
05 **B. Análise global**
08 **C. Destaques**
14 **D. Introdução**
17 **E. Ambiente sociotécnico**
19 O uso da Internet
20 Os usos de serviços críticos para a cibersegurança
23 Índice de ambiente sociotécnico
24 **F. Atitudes e comportamentos**
26 Confiança, segurança e privacidade - *smartphones*
29 Procedimentos de identificação utilizados nos serviços *online*
32 Privacidade e proteção dos dados pessoais
35 Democracia e cibersegurança
38 Administração Pública Central e Regional e Câmaras Municipais
45 Síntese - as atitudes e os comportamentos face à cibersegurança, em Portugal
46 **G. Sensibilização e educação**
47 Ações de sensibilização em cibersegurança
51 Sensibilização na Administração Pública Central e Regional e Câmaras Municipais
53 Cursos de Especialização Tecnológica e Cursos do Ensino Superior
55 Alunos inscritos e diplomados no ensino superior de cibersegurança
58 Síntese – a sensibilização e a educação sobre cibersegurança, em Portugal
59 **H. Briefing - Estratégia Nacional de Segurança do Ciberespaço**
62 **I. Recomendações**
63 **J. Notas conclusivas**
65 **K. Nota metodológica**
67 **L. Entidades parceiras do âmbito da Linha de Observação Sociedade**
68 **M. O Observatório de Cibersegurança do CNCS**
69 **N. Termos, siglas e abreviaturas**
72 **O. Referências principais**
76 **ANEXO – Linhas de ação da ENSC - Sociedade**

A. SUMÁRIO EXECUTIVO

Tal como nos anos anteriores, a terceira edição do *Relatório Cibersegurança em Portugal*, tema *Sociedade* analisa os indicadores mais recentes sobre as atitudes e os comportamentos face à cibersegurança, bem como a sensibilização e a educação nesta área. Em geral, refere-se a 2020 e considera, entre outros aspetos, o uso de *smartphones*, a gestão da privacidade, as ciberameaças à democracia, o setor público, as ações de sensibilização ou os cursos do ensino superior.

Os dados apresentados mostram que há um aumento da intensidade de uso e de utilizadores da Internet, bem como da utilização de alguns serviços críticos para a cibersegurança, como o *email* ou a banca *online*. Também se indicia que aquilo que os indivíduos percecionam e sabem relativamente à cibersegurança nem sempre coincide com os seus comportamentos. Não obstante, existem tendências razoavelmente positivas nos indivíduos. As organizações do setor público, por sua vez, têm-se adaptado progressivamente a algumas práticas de cibersegurança, mas têm falta de recursos. Quanto à sensibilização, apesar das sessões presenciais e à distância serem os tipos de ações predominantes, os cursos *online* gratuitos têm uma elevada capacidade de alcance de pessoas. O efeito destas ações (sessões e cursos) no comportamento das pessoas não é avaliado pela maioria das entidades organizadoras. No campo da educação, os números de cursos superiores de cibersegurança e segurança de informação e alunos inscritos e diplomados continuam a aumentar, mas ainda existe uma percentagem relativamente baixa de mulheres como alunas.

Alguns dos resultados apresentados neste documento são consequência direta do contexto de pandemia, particularmente importante em 2020, como é o caso do aumento do uso das videochamadas. Resta saber se no futuro voltaremos a valores pré-pandemia ou se alguns destes hábitos vieram para ficar.

Devido ao facto de as análises em causa se referirem, em geral, a um ano depois da aprovação da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENSC), optou-se por estabelecer algumas correspondências entre os indicadores apresentados e algumas linhas de ação promovidas pela ENSC, sobretudo referentes ao Eixo 2 - Prevenção, Educação e Sensibilização. Deste modo, contribui-se para uma das missões do Observatório de Cibersegurança, que é estudar o impacto da ENSC, e do Centro Nacional de Cibersegurança (CNCS), que é acompanhar a execução da mesma.

B._

ANÁLISE GLOBAL

TENDÊNCIAS – AMBIENTE SOCIOTÉCNICO

Verifica-se um crescimento na intensidade de uso e na quantidade de utilizadores da Internet, em Portugal, abrangendo alguns dos serviços mais críticos da ciber-higiene, como o *email*, as videochamadas, as mensagens instantâneas, as pesquisas de informação *online*, a banca *online* e o comércio eletrónico, destacando-se ainda a persistência de um uso muito elevado das redes sociais comparando com a média da União Europeia (UE).

TENDÊNCIAS – ATITUDES E COMPORTAMENTOS

As atitudes e os comportamentos nem sempre coincidem, isto é, por vezes aquilo que os indivíduos percecionam e sabem não corresponde ao que fazem, quer com paralelos positivos no comportamento, quer negativos, designadamente no uso de *smartphones*, do múltiplo fator de autenticação ou na gestão da privacidade. No entanto, os resultados apresentam tendência positiva. Existe alguma preocupação com o efeito do *online* na qualidade da democracia em termos de segurança e transparência, havendo uma grande exposição à desinformação, ainda que menor do que na média da UE. O setor público melhorou em vários aspetos da segurança das Tecnologias de Informação e Comunicação (TIC), mas ainda tem falta de recursos a este nível.

TENDÊNCIAS - SENSIBILIZAÇÃO E EDUCAÇÃO

Os cursos *online* massificados gratuitos de sensibilização para a cibersegurança têm um potencial de alcance de pessoas bastante elevado quando comparados com as sessões presenciais ou à distância. Todavia, existem atividades curriculares para os 1º, 2º e 3º ciclos de ensino que atingem uma grande população. As entidades que realizam ações de sensibilização tendem a não fazer uma avaliação da eficácia das suas estratégias no comportamento do seu público-alvo. Além disso, continua a verificar-se um aumento do número de cursos superiores de cibersegurança e segurança de informação, e de alunos inscritos e diplomandos, ainda que exista apenas uma licenciatura e um doutoramento e uma percentagem relativamente baixa de mulheres entre os alunos desta área.

O CASO COVID-19

A pandemia da Covid-19 marcou os anos de 2020 e 2021. Este acontecimento poderá explicar o maior uso da Internet e de certas plataformas, como as de videochamadas; a maior preo-

cupação com as ameaças à segurança e transparência da democracia resultantes de ciberameaças; a crescente necessidade de recursos de segurança das TIC por parte do setor público; e a particular relevância dos cursos *online* de sensibilização no que ao alcance de pessoas diz respeito.

ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO 2019-2023

Referindo-se este documento ao ano de 2020, dá-se início nesta série de relatórios sobre a componente "Sociedade" da cibersegurança ao acompanhamento de alguns indicadores de impacto da ENSC, sobretudo quanto ao Eixo 2 - Prevenção, Educação e Sensibilização. Relativamente às atitudes e comportamentos, os dados são razoáveis, isto é, pouco mais de metade dos indicadores disponíveis são positivos, quer em termos absolutos, quer se compararmos com a média da UE e considerarmos a evolução temporal. Contudo, verificam-se resultados piores em alguns grupos: entre as mulheres, na população sénior e relativamente a pessoas que estudaram menos anos. Os indicadores de educação e sensibilização também apresentam aspetos positivos em termos gerais na sua relação com a ENSC, sobretudo em termos de tendências, que são crescentes, mas o facto de existir apenas uma licenciatura e um doutoramento nesta área não favorece algumas das linhas de ação da ENSC.

C. DESTAQUES

Ambiente sociotécnico em Portugal, em 2020

Aumento do tráfego de dados fixos (ANACOM)

+ 55%
DO QUE EM 2019

Mais agregados familiares com ligação à Internet (INE)

+ 4
PP DO QUE EM 2019
(de 81% para 85%)

Mais utilizadores de Internet (INE)

+ 3
PP DO QUE EM 2019
(de 75% para 78%)

Mais uso do *email*, do telefone e videochamadas, das pesquisas *online*, da banca *online*, do comércio eletrónico, bem como manutenção de níveis elevados de uso das redes sociais (INE e Eurostat)

Comparando com 2019:

+ 3 PP EMAIL
(de 84% para 87%)

+ 18 PP TELEFONE E VIDEOCHAMADAS
(de 53% para 71%)

+ 1 PP PESQUISAS ONLINE
(de 86% para 87%)

+ 4 PP BANCA ONLINE
(de 56% para 60%)

+ 7 PP COMÉRCIO ELETRÓNICO
(de 28% para 35%)

80% UTILIZARAM REDES SOCIAIS
(65% em média na UE)

Confinamento social doméstico durante abril de 2020 atinge valores elevados (INE)

40%
DOS INDIVÍDUOS MANTIVERAM-SE NO MESMO LOCAL ONDE PERNOITARAM

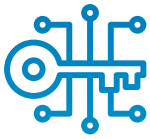
Atitudes e comportamentos em Portugal, em 2020

Sabe-se mais do que a média da UE da existência de sistemas de segurança nos *smartphones*, mas há menos cuidados (Eurostat)

90% **SABEM**
(84% na média da UE)

42% **JÁ RECUSARAM O ACESSO A DADOS PESSOAIS**
(52% em média na UE)

Aplica-se o múltiplo fator de autenticação mais do que a média da UE, mas também o acesso a plataformas através do *login* das redes sociais (Eurostat)



25% **JÁ USARAM PELO MENOS 4 MÉTODOS DE AUTENTICAÇÃO**
(22% em média na UE)

37% **USARAM LOGIN DAS REDES SOCIAIS**
(35% em média na UE)

Existe menos conhecimento sobre os *cookies*, mas faz-se a gestão dos dados pessoais *online* numa média superior à da UE (Eurostat)

59% **SABEM COMO FUNCIONAM OS COOKIES**
(69% em média na UE)

51% **LIMITA O ACESSO A PERFIL/CONTEÚDO DE REDES SOCIAIS**
(38% em média na UE)

Existe maior preocupação com as ciberameaças à democracia do que a média da UE (Eurobarómetro)

58% **TEM PREOCUPAÇÃO COM A POSSIBILIDADE DE CIBERATAQUES ÀS ELEIÇÕES**
(57% em média na UE)

Elevado nível de exposição à desinformação, mas menos do que a média da UE (Eurobarómetro)

39% (51% em média na UE)

Atitudes e comportamentos em Portugal, em 2020

Existe um perfil específico da pessoa com discurso mais consciente (Eurostat e Eurobarómetro)

HOMEM, JOVEM E COM FORMAÇÃO SUPERIOR TEM DISCURSO MAIS CONSCIENTE

Existem menos entidades da Administração Pública Central e Regional e Câmaras Municipais com estratégias de segurança de informação definidas (DGEEC)

61% **NO SEU CONJUNTO**
(- 6 pp do que em 2019)

Disponibilizam-se mais recomendações de segurança das TIC na Administração Pública Central e Regional e Câmaras Municipais, com uma subida acentuada de assuntos dedicados à formação (DGEEC)

45% **NO SEU CONJUNTO**
(+ 1 pp do que em 2019)

+36PP **NAS CÂMARAS MUNICIPAIS**
com o assunto da formação nessas recomendações

Existe uma elevada necessidade de profissionais de segurança das TIC na Administração Pública Central e Regional e Câmaras Municipais (DGEEC)

78% **DAS CÂMARAS MUNICIPAIS**
têm esta necessidade
(+ 23 pp do que em 2019)

Educação e Sensibilização em Portugal, em 2020

A maioria das ações de sensibilização realizadas são sessões presenciais e à distância (CNCS)

99%
SÃO SESSÕES PRESENCIAIS E À DISTÂNCIA

Muitas das ações de sensibilização são integradas em atividades curriculares em todo o ensino não superior (CNCS)

1º | 2º | 3º
CICLOS DE ENSINO

Os cursos *online* de sensibilização gratuitos são ações que têm um elevado alcance de pessoas em comparação com as sessões presenciais e à distância (CNCS)

21% **DAS PESSOAS ALCANÇADAS**

A maior parte das entidades que realizam ações de sensibilização não avaliam os seus resultados nos comportamentos das pessoas (CNCS)

75% **NÃO AVALIAM**

A maioria das entidades da Administração Pública Central e Regional e Câmaras Municipais não realizam ações de sensibilização obrigatórias mas sim voluntárias (DGEEC)

22% **TÊM AÇÕES OBRIGATÓRIAS**

Educação e Sensibilização em Portugal, em 2020

Regista-se mais uma vez um aumento no número de cursos superiores de cibersegurança e segurança de informação (CNCS)

Comparando com 2019-2020:

+3
TESP

+1
MESTRADO

Apenas existe uma licenciatura e um doutoramento em cibersegurança e segurança de informação (CNCS)

1 (=)
LICENCIATURA

1 (=)
DOUTORAMENTO

Regista-se um aumento no número de alunos e diplomados nos cursos superiores de cibersegurança e segurança de informação (CNCS)

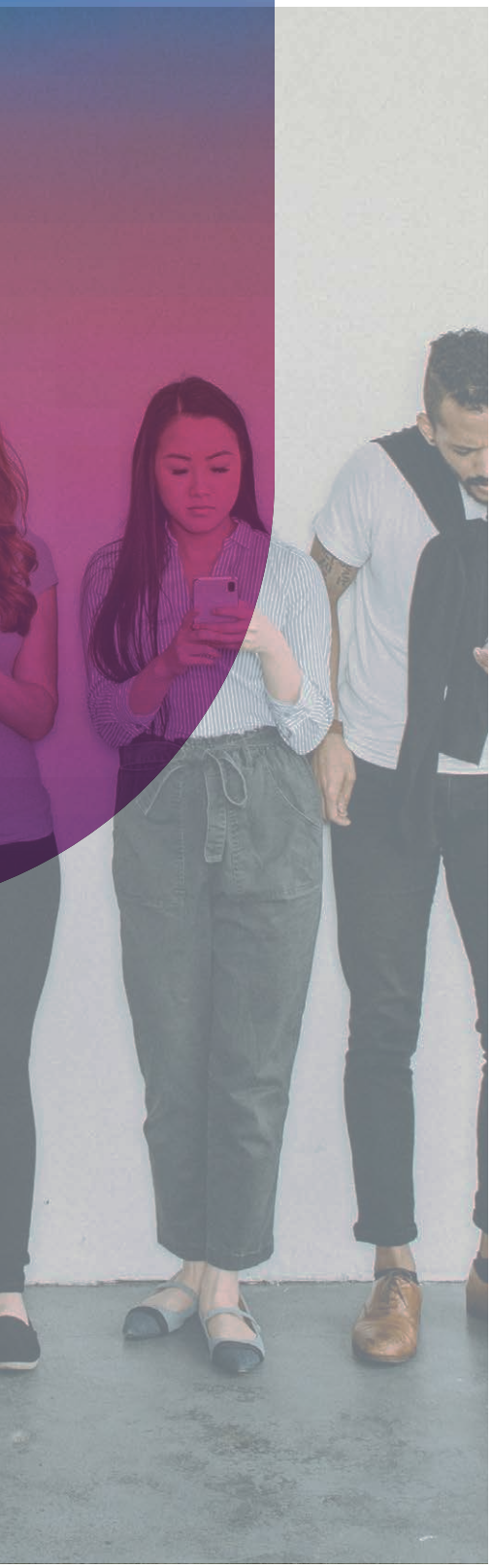
+13% **DE INSCRITOS**
(face a 2019-2020)

+103% **DE DIPLOMADOS**
(face a 2018-2019)

A percentagem de mulheres diplomadas e inscritas nos cursos superiores de cibersegurança e segurança de informação continua a ser relativamente baixa (CNCS)

8% **DE INSCRITAS**
(+ 1 pp do que em 2019- 2020)

9% **DE DIPLOMADAS**
(+ 5 pp do que em 2018-2019)



D. INTRODUÇÃO

O *Relatório Cibersegurança em Portugal* - tema *Sociedade 2021* é a terceira edição desta publicação anual dedicada aos aspetos socias da cibersegurança. Esta análise, incidindo em dados disponíveis até 2020, cobre com particular enfoque o período da pandemia da Covid-19 que assolou Portugal e o mundo, e que ainda persiste. Esta circunstância interfere com os resultados deste estudo, nomeadamente porque é visível que certas tendências acentuadas terão correlação com o confinamento social e as mudanças comportamentais promovidas pelas restrições às interações presenciais. Contudo, não é líquido que estas dinâmicas sejam invertidas assim que a situação pandémica seja mais controlada ou totalmente superada. As mudanças sociais aparentemente circunstanciais podem por vezes instalar-se como hábitos permanentes.

No contexto da crescente digitalização promovida por processos anteriores à pandemia, mas intensificados por esta, a cibersegurança ganhou notoriedade, em particular enquanto esfera de mitigação dos potenciais efeitos negativos de uma transição digital acelerada e, assim, de um incremento da exposição à Internet. Nesta conjuntura, o CNCS, na sua conferência C-Days 2021, utilizou como mote "naturalizar competências", isto é, apelou à necessidade de tornar as boas práticas de cibersegurança em mais um conteúdo entre as aprendizagens dos mais jovens, de modo a fazer parte dos instrumentos básicos fornecidos aos indivíduos na socialização primária. Só assim será possível ultrapassar a iliteracia digital que ainda existe relativamente à cibersegurança e outras competências digitais (EC, 2021).

O presente documento do Observatório de Cibersegurança do CNCS dá continuidade ao estudo, realizado nos relatórios anteriores com o mesmo tema, sobre as atitudes, os comportamentos, a sensibilização e a educação face a esta área. Alguns

indicadores apresentados nos últimos dois relatórios não têm continuidade neste, como os do Eurobarómetro Especial sobre Cibersegurança, devido ao facto de não terem sido publicados este ano. Não obstante, outros são utilizados pela primeira vez, como os que se referem ao Eurobarómetro Especial sobre a Democracia na UE. Estas mudanças fazem com que a metodologia para a análise global utilizada na edição de 2020 não seja aplicada do mesmo modo neste número e que se evite uma comparação direta com a mesma (a qual poderá ser feita assim que os indicadores análogos do ano passado estejam disponíveis). Esta limitação não obsta a que se façam observações em linha temporal e comparações com 2019.

Neste relatório também se aprofunda o inquérito realizado pelo CNCS às entidades consideradas chave na realização de ações de sensibilização para a ciber-higiene, iniciando-se uma série sobre a eventual avaliação que estas entidades fazem do impacto das suas ações no comportamento dos seus públicos-alvo. Este documento traz ainda como novidade a articulação entre os indicadores apresentados e as linhas de ação da ENSC correlacionadas, de modo a encetar um acompanhamento mais constante do Observatório de Cibersegurança relativamente aos potenciais impactos da ENSC.

Certos indicadores de uso do ciberespaço, não dizendo explicitamente respeito à cibersegurança, são fundamentais para compreender um ambiente digital que pode conduzir a práticas menos seguras. Foi por esta razão que se introduziu nesta edição um capítulo sobre o que se designa de "ambiente sociotécnico", no qual se analisam os usos da Internet e de algumas plataformas tidas como críticas para a cibersegurança.

O documento é divido em quatro capítulos principais relativos a indicadores e análise de resultados: o referido Ambiente Sociotécnico, onde se mostram dados sobre o uso de tecnologias digitais, articulando-se com os serviços mais críticos, como o *email*, as videochamadas ou o banco *online*, entre outros; Atitudes e Comportamentos, com indicadores sobre perceções, conhecimentos e hábitos dos indivíduos quanto à cibersegurança, mas também de organizações do setor público; Sensibilização e Educação, no qual se analisam as ações de sensibilização realizadas e a evolução dos cursos superiores explicitamente desta área; e, por fim, o Briefing - Estratégia Nacional de Segurança do Ciberespaço, através do qual se aprofundam as articulações hipotéticas entre as linhas de ação da ENSC referentes à componente social e os indicadores evidenciados neste documento. Por fim, nos restantes capítulos, apresentam-se algumas recomendações, as notas conclusivas, a metodologia, as entidades parceiras envolvidas neste relatório, o Observatório de Cibersegurança, uma lista

de termos, siglas e abreviaturas e as referências principais. No anexo é possível encontrar por fim um quadro com a identificação das linhas de ação da ENSC em análise.

1.
AMBIENTE SOCIOTÉCNICO

O ano 2020 é marcado pelo emergir da pandemia da Covid-19 e pela mudança social, económica e tecnológica que a mitigação dos riscos do vírus associado a esta doença acarretou. A rápida conversão ao trabalho remoto de muitas atividades resultou num aceleramento do recurso ao digital bem visível nos números e no ambiente sociotécnico[1]. A cibersegurança nem sempre foi considerada com a devida relevância no contexto desta conversão, quer devido à falta de tempo e recursos de quem se converteu de forma reativa, quer porque poderá ter sido esquecida no meio das necessidades da digitalização em curso.

O significativo aumento no número de incidentes de cibersegurança e nos indicadores de cibercrime em 2020 e a sua correlação com os vários confinamentos sociais (CNCS, 2021) acabaram por colocar a cibersegurança também no centro das preocupações entre as vozes que falam em nome do tecido económico, nomeadamente no espaço mediático, mas também no âmbito da criação de políticas públicas orientadas ao desenvolvimento digital.

A preparação e a adaptação ao trabalho remoto realizaram-se de forma assimétrica. As grandes empresas e as pessoas com mais formação e recursos económicos puderam beneficiar de condições de partida mais favoráveis para um melhor acesso a equipamentos e a espaços de trabalho (Silva *et al*., 2020). Estes fatores ajudam a interpretar as desigualdades na adoção da cibersegurança como serviço e como competência. Quanto maior o capital educacional, maior a capacidade para aplicar as melhores práticas de segurança na Internet e no uso das tecnologias digitais (CNCS, 2020). A vulnerabilidade social é frequentemente também uma vulnerabilidade de segurança, sobretudo quando se refere ao utilizador individual e às burlas em contexto digital, aspeto tão relevante nos números sobre os riscos e os conflitos de 2020 (CNCS, 2021). As pequenas e médias empresas também entram nesta equação. Os dados mostram que estas têm menos maturidade em cibersegurança comparando com as grandes empresas (CNCS, 2020) e, talvez por isso, são igualmente alvo de ciberataques, como, por exemplo, de *ransomware*. Esta situação poderá não se dever apenas à falta de recursos, mas também à falta de consciência por parte dos empresários.

O volume e a intensidade de uso das tecnologias digitais são indicadores fundamentais para perceber o grau de exposição aos riscos no ciberespaço, aspeto que terá de ser articulado com os níveis de literacia e de maturidade em cibersegurança por parte de indivíduos e organizações.

1 "Ambiente sociotécnico" é entendido neste âmbito como referência aos indicadores de usos de tecnologias com destaque para as suas implicações sociais num dado contexto.

O USO DA INTERNET

No que diz respeito ao uso da Internet, fator central para compreender o acesso ao ciberespaço, os números disponíveis mostram um claro aumento. De acordo com a Autoridade Nacional de Comunicações (ANACOM), o tráfego de dados fixos registou um crescimento de 55% em 2020 face a 2019, estimando-se que este crescimento, considerando a tendência histórica, teria sido apenas de 19% caso não tivesse ocorrido a pandemia da Covid-19 (ANACOM, 2021)[2]. Segundo o Instituto Nacional de Estatística (INE), a proporção de agregados familiares com ligação à Internet aumentou 4 pontos percentuais (pp), de 81% em 2019 para 85% em 2020 (INE, 2020a). É referido no mesmo documento do INE que "é preciso recuar a 2016 para se observar um aumento anual mais expressivo no acesso à Internet e à banda larga em casa" (2020a: p.16). Nos três meses anteriores às entrevistas realizadas[3] (entre abril e agosto de 2020 – coincidindo com o primeiro confinamento), a proporção de utilizadores de Internet subiu 3 pp, de 75% no período homólogo para 78% em 2020, "contrariando a estabilidade dos resultados nos dois anos anteriores", refere o INE (2020a: p.16). Na UE esse aumento foi de 2 pp, de 86% para 88% - portanto, representando valores totais mais elevados do que os registados em Portugal (Eurostat, 2020a).

Significativo é o facto de a proporção de empresas com 10[4] ou mais trabalhadores que utilizam computadores com ligação à Internet para fins profissionais ter diminuído de 98% em 2019 para 97% em 2020, algo em parte explicável pelo alto volume dos valores em causa, menos propensos a subidas, mas também, eventualmente, pela transição dos processos de trabalho para o espaço doméstico provocada pela pandemia. Já a percentagem de pessoas ao serviço que utilizam um computador com ligação à Internet para fins profissionais cresceu 5 pp de 38% em 2019 para 43% em 2020 (INE, 2020b).

Portanto, os dados mostram um aumento na intensidade de uso e no número de pessoas que usam a Internet, logo, uma maior exposição às vulnerabilidades e aos riscos do ciberespaço. O facto desta tendência ser mais significativa em pessoas com mais formação pode ser um elemento que atenue essa exposição, na medida em que estes indivíduos mostram ter uma maior consciência relativamente aos riscos do ciberespaço, pelo menos no que se refere ao discurso.

2 Todos os valores indicados neste documento são apresentados de forma arredondada.

3 Os dados do INE e do Eurostat em relação a indivíduos apresentados nesta secção dizem respeito ao intervalo etário entre os 16 e os 74 anos de idade e a utilizações da Internet ou compras *online* nos últimos 3 meses. As exceções são identificadas no corpo do texto.

4 Subtraindo as empresas financeiras.

OS USOS DE SERVIÇOS CRÍTICOS PARA A CIBERSEGURANÇA

Do ponto de vista da ciber-higiene, existem alguns serviços críticos que interessa considerar, de modo a, também aí, se avaliarem os níveis de exposição ao risco. Verifica-se nestes casos a mesma tendência de subida identificada em relação ao uso da Internet. Vejamos alguns valores no que diz respeito a esses serviços críticos e a sua articulação com as ciberameaças existentes.

EMAIL:

Dados relevantes: verifica-se um crescimento do uso de *email* (receção e envio) em 3 pp, de 84% em 2019 para 87% em 2020, entre os indivíduos em Portugal. A média da UE manteve-se igual ao ano anterior, com 85% (INE, 2020a; Eurostat, 2020b).

Aspetos críticos: pelo *email* ocorrem atividades maliciosas como o *phishing*, a distribuição de *malware*, a fraude/burla, ciberameaças muito importantes em geral e no ano de 2020 em particular (CNCS, 2021).

OUTRAS FORMAS DE COMUNICAÇÃO PELA INTERNET (VIDEOCHAMADAS E MENSAGENS INSTANTÂNEAS):

Dados relevantes: telefonar ou fazer videochamadas em Portugal aumentou 18 pp, de 53% dos indivíduos em 2019 para 71% em 2020. A média da UE acompanhou esta tendência, subindo 8 pp, de 62% para 70%. A troca de mensagens instantâneas é das atividades mais intensas, praticada por 90% dos respondentes em 2020, mais 4 pp do que em 2019, com 86% (INE, 2020a; Eurostat, 2020b).

Aspetos críticos: as videochamadas colocam desafios sobretudo ao nível da partilha de dados pessoais e dados sensíveis, nomeadamente quando existe alguma exposição presente na imagem de fundo ou quando não são seguidos os procedimentos básicos de ciber-higiene e ocorrem intrusões. Além disso, a gravação de imagens pode ser aproveitada para a produção de *deep fakes*. As mensagens instantâneas, por sua vez, são plataformas através das quais podem ocorrer ataques de *phishing* e a disseminação de desinformação.

REDES SOCIAIS:

Dados relevantes: a participação em redes sociais em 2020 em Portugal manteve os valores de 2019, em 80% dos indivíduos. A média da UE aumentou 2pp, de 63% para 65%. Portanto, verifica-se que Portugal apresenta um uso das redes sociais muito superior à média da UE, uma diferença de 15 pp (INE, 2020a; Eurostat, 2020b).

Aspetos críticos: pelas redes sociais ocorrem práticas particularmente ligadas à engenharia social, como a desinformação, o roubo de identidade, o *phishing*, a burla/fraude e a criação de perfis de utilizadores para fins maliciosos.

NAVEGAÇÃO:

Dados relevantes: pesquisar informação sobre produtos ou serviços, pelos indivíduos em Portugal, aumentou cerca de 1 pp, de 86% em 2019 para 87% em 2020. A média da UE cresceu 3 pp, de 77% para 80%. Tal como na participação em redes sociais, Portugal, neste domínio, apresenta números superiores à média da UE, com mais 7 pp. Curiosamente, a pesquisa sobre informações relativas à saúde diminuiu, presente em 66% dos indivíduos em 2019 e em 63% em 2020. A média da UE, a este respeito, cresceu de 62% para 64% no mesmo período (INE, 2020a; Eurostat, 2020b).

Aspetos críticos: a navegação, em particular a pesquisa de informação sobre produtos ou serviços, entre outros, se não realizada com todos os cuidados, pode conduzir os internautas a *websites* maliciosos, que instalem *malware* nos dispositivos, capturem dados pessoais ou que promovam fraudes/burlas através de esquemas com produtos e serviços.

BANCA ONLINE:

Dados relevantes: o uso de serviços de banca *online* pelos indivíduos cresceu 4 pp em Portugal, de 56% em 2019 para 60% em 2020. A média da UE, por sua vez, subiu 2 pp, de 64% para 66% (INE, 2020a; Eurostat, 2020b).

Aspetos críticos: a banca *online* é um ponto crítico porque o roubo de credenciais e de identidade podem conduzir a acessos e usos ilegítimos em relação a serviços bancários. Muitos dos casos de *phishing* existentes procuram a captura deste tipo de dados. A instalação de aplicações neste contexto deve ser feita também com particular cuidado, de forma a evitar plataformas fraudulentas.

COMÉRCIO ELETRÓNICO:

Dados relevantes: registou-se o aumento mais significativo em Portugal desde que esta série de indicadores foi iniciada, em 2002, verificando-se em 2020 mais 7 pp do que 2019 no que se refere a pessoas que utilizaram o comércio eletrónico, passando de 28% para 35% do total. A média da UE em relação a este indicador subiu 5 pp, de 49% para 54% (INE, 2020a; Eurostat, 2020c).

Aspetos críticos: o comércio eletrónico é um ponto crítico porque é através desta prática que ocorrem burlas *online* com produtos fraudulentos ou fraudes através da plataforma MBWay, sobretudo por utilização incorreta. Também é mediante *websites* de comércio eletrónico que ocorre o chamado "*online skimming*", isto é, a captura de dados de cartões de crédito em páginas de venda de produtos *online* que apresentam vulnerabilidades de segurança.

O TRABALHO REMOTO:

Dados relevantes: 31% dos indivíduos em Portugal, com emprego, afirmaram que utilizaram as TIC para exercer a sua profissão em casa no mês anterior à entrevista, entre abril e agosto de 2020, dos quais 98% usaram o *email* e 83% uma plataforma de videoconferência. De referir que, destes 31%, cerca de 57% tinham o ensino superior (INE, 2020a). Outros dados mostram que em abril de 2020, momento do primeiro confinamento, entre as pessoas com dispositivos ligados à Internet, em média, 40% mantiveram-se no mesmo local onde pernoitaram (INE, 2021) e em média mantiveram-se em casa mais 30% de indivíduos do que antes da pandemia (GE-METD, 2021).

Aspetos críticos: o trabalho remoto coloca os indivíduos em contexto de maior isolamento social, de eventual menor interação com os responsáveis pela segurança das TIC das suas organizações e sem os adequados mecanismos de segurança, aumentando o potencial para o sucesso de ciberataques através de engenharia social ou que explorem vulnerabilidades em serviços remotos, por exemplo.

ÍNDICE DE AMBIENTE SOCIOTÉCNICO

Internet em 2020 – aumento de intensidade de uso e de quantidade de utilizadores.

Aspetos críticos em 2020 – crescimento no volume de usos de *email*, videochamadas, mensagens instantâneas, pesquisas de informação *online*, banca *online* e comércio eletrónico, bem como intensificação do trabalho remoto.

Particular destaque para o aumento de volume de videochamadas e para o facto de as redes sociais, ainda que não tenham visto o seu uso crescer em relação ao ano anterior, serem muito mais usadas em Portugal do que a média da UE.

F

ATITUDES E COMPORTAMENTOS

Relativamente a atitudes e comportamentos, existem importantes ausências em termos de indicadores disponíveis, sobretudo se considerarmos que este ano não foi lançado o Eurobarómetro acerca das atitudes dos europeus face à cibersegurança. Acresce que alguns indicadores de cibersegurança no âmbito dos Inquéritos à Utilização das Tecnologias da Informação e Comunicação nas Empresas e pelas Famílias, do INE, não foram aplicados.

Não obstante, é possível recolher alguns indicadores sobre matéria comportamental bastante relevantes e, em alguns casos, novidades em relação ao ano anterior. A cibersegurança relaciona-se de modo muito direto com as formas de proteção da privacidade e os processos de construção da identidade *online*. A privacidade protegida e a identidade autêntica são frequentemente bens que a cibersegurança procura manter intactos. Além disso, a perceção que os indivíduos constroem do mundo é cada vez mais definida pelo ambiente do ciberespaço, algo que pode ser afetado perniciosamente pela desinformação, tendo implicações na qualidade da democracia e na cibersegurança.

Estes serão alguns dos aspetos analisados neste capítulo, que se divide em cinco subcapítulos temáticos considerando os indicadores disponíveis no momento de construção deste documento e os assuntos que são tidos como importantes no contexto atual: Confiança, segurança e privacidade - *smartphones*; Procedimentos de identificação utilizados nos serviços *online*; Privacidade e proteção dos dados pessoais; Democracia e cibersegurança; e Administração Pública Central e Regional e Câmaras Municipais. No final de cada conjunto de indicadores destacados indicam-se as linhas de ação da ENSC com as quais aqueles se relacionam. Para identificar cada linha de ação, consultar o anexo. No final do relatório será feita uma análise mais detalhada sobre a relação entre estes indicadores e a ENSC.

CONFIANÇA, SEGURANÇA E PRIVACIDADE - SMARTPHONES

O inquérito do Eurostat (2020d) Confiança, segurança e privacidade - *smartphones* [*Trust, security and privacy – smartphones*] analisa alguns aspetos sobre a relação de confiança que os utilizadores estabelecem com o seu *smartphone*. O momento de aplicação do questionário em Portugal decorreu entre abril e agosto de 2020, reportando aos usos durante os últimos 3 meses. Por isso, os dados incidem em particular sobre o primeiro confinamento resultante da pandemia da Covid-19. Destacam-se os seguintes indicadores:

Confiança, segurança e privacidade - *smartphones*, em Portugal e na média da UE, 2020, últimos 3 meses, *indivíduos* (%)

Figura 1 | Eurostat, 2020d

Se considerarmos os aspetos correlacionados com as atitudes, isto é, com os valores, opiniões e conhecimentos face à cibersegurança, verificamos que em Portugal existem menos indivíduos a afirmar que não sabem se o *smartphone* tem algum sistema de segurança (10%) do que a média da UE (16%). Também existem menos indivíduos em Portugal que não sabem que é possível restringir ou recusar o acesso a dados pessoais, quando usaram ou instalaram uma aplicação (4%), comparando com a média da UE (6%).

Quanto aos comportamentos, isto é, aquilo que os indivíduos fazem, os dados relativos a Portugal aparecem numa posição mais negativa, comparando com os níveis de conhecimento assumidos e com a média da UE. Por exemplo, em Portugal, 23% dos indivíduos afirmam que o seu *smartphone* tem algum sistema de segurança instalado automaticamente ou providenciado com o sistema operativo, portanto, por defeito, quando a média da UE é de 39%. Estes dados devem ser lidos como representando em parte uma realidade material, mas também como resultando de perceções que os próprios indivíduos têm sobre o seu dispositivo móvel. Os dispositivos móveis têm, em geral, pelo menos alguma aplicação de segurança por defeito, mesmo que os utilizadores não o reconheçam. Quanto a sistemas de segurança instalados por alguém ou subscritos no *smartphone*, isto é, sem ser por defeito, os números no país coincidem com a média da UE, em 11%. Questionados sobre se praticaram alguma ação que restringe ou recusa o acesso a dados pessoais de uma aplicação instalada no seu *smartphone*, em Portugal apenas 12% dos indivíduos admitem tê-lo feito, enquanto a média da UE é de 18%.

Por fim, é possível salientar que, embora em termos de ações positivas, os indivíduos em Portugal apresentem indicadores mais negativos do que as médias da UE, são em Portugal menos aqueles que admitem ter perdido informações, documentos, fotos ou outro tipo de dados no *smartphone* em resultado de um vírus ou programa hostil, com 2%, quando a média da UE atinge os 4%. Esta diferença pode significar que os indivíduos, embora tenham menos cuidados ao nível dos comportamentos, também se sentiram menos vítimas de ameaças no ciberespaço ou têm menos competências para as reconhecer (Eurostat, 2020d).

Aspetos sociodemográficos relevantes em Portugal, 2020

Sexo	**Os indivíduos do sexo masculino tendem a apresentar valores ligeiramente mais positivos.** Por exemplo, 13% afirmam ter algum sistema de segurança no seu *smartphone* sem ser por defeito, enquanto as pessoas do sexo feminino atingem apenas os 9%.
Idade	**Os jovens tendem a ter mais cuidados do que os seniores.** Por exemplo, 12% das pessoas com idades compreendidas entre os 16 e os 24 anos afirmam ter algum sistema de segurança no seu *smartphone* sem ser por defeito, enquanto apenas 4% das pessoas com idades entre os 65 e os 74 o reconhecem.
Educação	**As pessoas com uma educação formal elevada tendem a afirmar ter mais cuidados do que as que possuem uma educação formal baixa.** Por exemplo, 16% das pessoas com educação formal superior afirmam ter algum sistema de segurança no seu *smartphone* sem ser por defeito, enquanto apenas 8% dos indivíduos com educação formal básica o afirmam (idades entre os 25 e os 64 anos).
UE	Valores genericamente alinhados com a média da UE.

DESTAQUES

Em Portugal, existem menos indivíduos do que na média da UE a não saberem se existe algum sistema de segurança nos seus *smartphones* e se é possível restringir o acesso das aplicações aos dados pessoais.

Ao nível do comportamento, em Portugal os indivíduos tendem a ter menos cuidados de segurança com o *smartphone* do que a média da UE.

As pessoas do sexo masculino, os jovens e as pessoas com formação superior afirmam ter mais cuidados de segurança com o *smartphone* do que as pessoas do sexo feminino, os seniores e aqueles que têm uma formação básica.

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

PROCEDIMENTOS DE IDENTIFICAÇÃO UTILIZADOS NOS SERVIÇOS ONLINE

Um outro inquérito publicado pelo Eurostat (2020e) - Procedimentos de identificação utilizados nos serviços *online* [*Identification procedures used for online services*] - é igualmente relevante para analisar o domínio das atitudes e comportamentos face à cibersegurança. Neste caso, a informação incide sobre os métodos utilizados pelos indivíduos para autenticarem a sua identidade no acesso aos serviços *online*, aspeto que se relaciona com um dos elementos mais críticos da ciber-higiene: o uso de palavra-passe e o múltiplo fator de autenticação.

Procedimentos de identificação utilizados nos serviços *online*, em Portugal e na média da UE, 2020, últimos 3 meses, *indivíduos* (%)

Figura 2 | Eurostat, 2020e

O procedimento de identificação mais comum é o que utiliza um *login* simples através do nome do utilizador e palavra-passe para aceder a serviços *online*. Em Portugal, 60% dos inquiridos utilizam este método, enquanto a média da UE atinge os 73%. Existe adicionalmente um conjunto de indicadores relativamente a procedimentos que em geral se associam ao uso de nome de utilizador e palavra-passe, configurando um múltiplo fator de autenticação e conferindo uma camada adicional de segurança: o uso de *token* - 37% em Portugal e 35% na média da UE; ou o uso de mensagem de telemóvel - 46% em Portugal e 45% na média da UE. Em relação a estes indicadores, Portugal apresenta-se, portanto, ligeiramente acima da média da UE. De realçar também o uso de certificado de identificação eletrónica, também por vezes associado a uma palavra-passe, ou o uso de leitor de cartões, que em Portugal são utilizados apenas por 10% dos inquiridos, enquanto a média da UE chega aos 20%. Um procedimento particularmente desaconselhado é a utilização do *login* das redes sociais para aceder a outros serviços *online*, devido à potencial partilha de dados, algo que em Portugal, com 37%, se pratica mais do que na média da UE, com 35%. Os inquiridos em Portugal utilizaram pelo menos 4 dos procedimentos descritos num volume de 25%, enquanto a média da UE é de 22%.

Estes dados mostram que, por um lado, os indivíduos em Portugal utilizam procedimentos associados ao uso de múltiplos fatores de autenticação num volume um pouco acima da média da UE. Mas, por outro, também revelam que se utiliza demasiado o *login* através das redes sociais a outros serviços *online* e pouco os certificados de identificação eletrónica ou leitores de cartões (Eurostat, 2020e).

Aspetos sociodemográficos relevantes em Portugal, 2020

Sexo **Em geral, os indivíduos do sexo feminino tendem a utilizar menos os procedimentos de identificação e aqueles com maior complexidade do que os do sexo masculino.** Por exemplo, 21% das mulheres utilizaram pelo menos 4 dos procedimentos descritos, enquanto entre os homens o volume é de 29%.

Idade **Os indivíduos seniores utilizam menos procedimentos de identificação e com menos complexidade do que os mais jovens.** Por exemplo, apenas 4% dos indivíduos com idades entre os 65 e os 74 anos utilizaram pelo menos 4 dos procedimentos descritos, enquanto as pessoas entre os 16 e os 24 anos atingem os 31%.

Educação **Os indivíduos com educação formal baixa utilizam menos procedimentos de identificação e com menos complexidade do que os que têm uma educação formal elevada.** Por exemplo, apenas 8% dos indivíduos com educação básica utilizaram pelo menos 4 dos procedimentos descritos, enquanto os que têm uma educação superior chegam aos 50% (idades entre os 25 e 64 anos).

UE Valores genericamente alinhados com a média da UE.

DESTAQUES

Em Portugal, os indivíduos utilizam o múltiplo fator de autenticação em volume ligeiramente acima da média da UE.

Existe uma utilização acima da média da UE do *login* das redes sociais para acesso a outros serviços *online*.

Verifica-se uma baixa utilização de certificados digitais ou leitores de cartões como procedimentos de identificação *online*, comparando com a média da UE.

Os indivíduos do sexo masculino, os mais novos e aqueles que possuem formação mais elevada tendem a utilizar mais procedimentos de identificação de serviços *online* e mais complexos.

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

PRIVACIDADE E PROTEÇÃO DOS DADOS PESSOAIS

Relativamente à privacidade e proteção de dados, o Eurostat (2020c) publicou um conjunto de indicadores - Privacidade e proteção de dados pessoais [*Privacy and protection of personal data*] - que se afiguram com alguma relevância para monitorizar o nível de cuidado que os utilizadores têm com os seus dados pessoais quando navegam *online* ou quando instalam aplicações.

Privacidade e proteção dos dados pessoais, em Portugal e na média da UE, 2020, últimos 3 meses, *indivíduos* (%)

Figura 3 | Eurostat, 2021f

No que diz respeito ao conhecimento sobre o funcionamento dos *cookies*, em Portugal, 59% dos indivíduos afirmam saber que os *cookies* podem ser usados para rastrear movimentos de pessoas na Internet. A média da UE é superior em 10 pp, com 69%. Também há menos indivíduos em Portugal do que na média da UE a terem alterado as configurações do *browser* para evitar ou limitar os *cookies* em qualquer um dos seus dispositivos, no valor de 28%, contra 32% da média da UE. Acresce que em Portugal há menos indivíduos a utilizarem *software* que limita a capacidade de rastreamento das suas atividades na Internet, com um volume de 14%, contra 17% de média na UE.

Estes resultados abaixo da média da UE acerca de *cookies* e do rastreamento são compensados pelos que dizem respeito à gestão dos dados pessoais na Internet. Portugal surge sempre acima das médias da UE nesta matéria: com mais indivíduos a lerem as declarações de política de privacidade antes de fornecerem os seus dados pessoais – 41% em Portugal e 40% na média da UE; com mais indivíduos a restringirem ou recusarem o acesso à sua localização geográfica – 54% em Portugal e 44% na média da UE; com mais indivíduos a limitarem o acesso a perfil ou conteúdo em *websites* de redes sociais ou de armazenamento *online* partilhado - 51% em Portugal e 38% na média da UE; com mais indivíduos a recusarem o uso de dados pessoais para fins publicitários – 52% em Portugal e 49% na média da UE; e com mais indivíduos a verificarem se o *website* a que os seus dados pessoais são fornecidos é seguro – 44% em Portugal e 32% na média da UE.

Aspetos sociodemográficos relevantes em Portugal, 2020

Sexo **Os indivíduos do sexo feminino tendem a ter menos cuidados relativamente à privacidade e proteção de dados** *online* **do que os do sexo masculino.** Por exemplo, 70% dos homens já aplicaram pelo menos uma das medidas de gestão do acesso aos dados pessoais descritas, enquanto entre as mulheres o valor é de 66%.

Idade **Os indivíduos seniores tendem a ter menos cuidados relativamente à privacidade e proteção de dados** *online* **do que os jovens.** Por exemplo, enquanto 96% dos indivíduos com idades compreendidas entre os 16 e os 24 anos já aplicaram pelo menos uma das medidas de gestão do acesso aos dados pessoais descritas, apenas 26% das pessoas com idades entre os 65 e 74 anos o fizeram.

Educação **Os indivíduos com formação básica tendem a ter menos cuidados relativamente à privacidade e proteção de dados** *online* **do que os que têm uma formação superior.** Por exemplo, 96% dos indivíduos com formação superior já aplicaram pelo menos uma das medidas de gestão do acesso aos dados pessoais descritas e apenas 47% dos que têm formação básica afirmam o mesmo.

UE Valores genericamente alinhados com a média da UE.

Destaques

Os indivíduos em Portugal têm menos conhecimento e comportamentos menos cuidadosos do que a média da UE relativamente à função e ao uso dos *cookies*.

Não obstante, os indivíduos em Portugal apresentam valores acima das médias da UE no que diz respeito à aplicação de práticas de gestão dos dados pessoais na Internet.

Mais uma vez, o perfil do indivíduo mais cuidadoso, neste caso em matéria de privacidade e proteção de dados pessoais, tende a ser homem, jovem e com estudos superiores.

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

DEMOCRACIA E CIBERSEGURANÇA

O Eurobarómetro, embora não tenha lançado em 2020 o inquérito especial sobre cibersegurança, aplicou um outro sobre a democracia na UE, através do qual trata algumas questões ligadas diretamente à cibersegurança. Estas questões analisam as atitudes e os comportamentos dos cidadãos face às ameaças que o ciberespaço pode colocar ao ambiente democrático (Eurobarómetro, 2020).

Uma das questões que importa considerar é sobre se os indivíduos, no contexto das eleições na Europa, estão preocupados com a possibilidade de as eleições serem manipuladas por meio de ciberataques.

Nível de preocupação com a possibilidade de as eleições serem manipuladas por meio de ciberataques, em Portugal e na média da UE, 2018 e 2020, *indivíduos* (%)

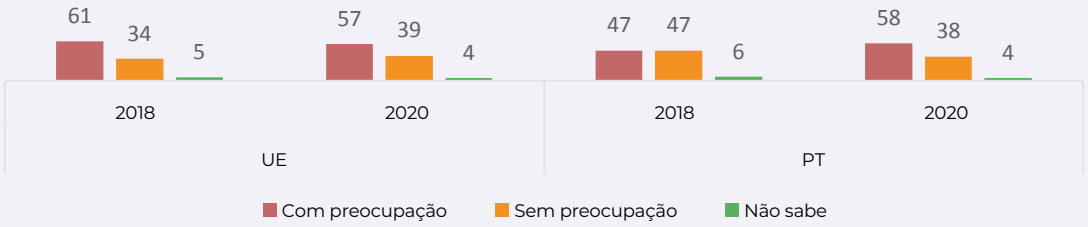


Figura 4 | Eurobarómetro, 2020

Como é possível verificar, a percentagem de indivíduos em Portugal a manifestar esta preocupação aumentou para 58%, uma subida de 11 pp em relação ao último inquérito, de 2018. Este valor surge 1 pp acima da média da UE. A tendência em Portugal é inversa à da UE, visto neste caso ter havido uma descida de 61% em 2018 para 57% em 2020, menos 4 pp.

Nível de preocupação com o potencial para fraude ou ciberataque, caso pudesse votar eletronicamente, online ou por via postal, em Portugal e na média da UE, 2018 e 2020, *indivíduos* (%)

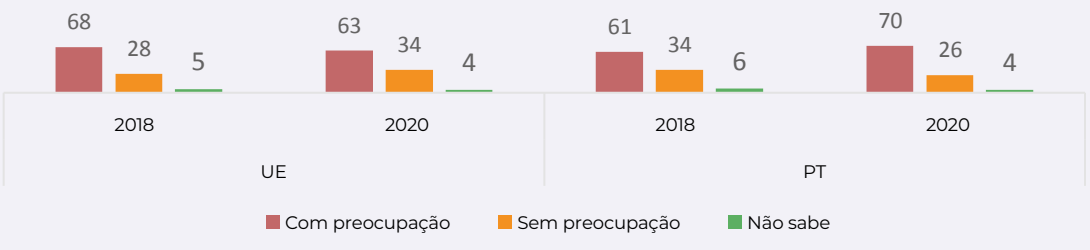


Figura 5 | Eurobarómetro, 2020

Quando questionados sobre se a possibilidade da aplicação do voto eletrónico conduz à preocupação com a fraude ou um ciberataque, 70% dos indivíduos em Portugal manifestam algum tipo de preocupação, enquanto a média da UE apresenta menos 7 pp, com 63%. Estes valores representam, em relação a 2018, uma subida para Portugal, em 9 pp, e uma descida para a média da UE, em 5 pp.

Indivíduos que afirmam já ter sido expostos ou testemunhado pessoalmente alguma das seguintes situações, em Portugal e na média da UE, 2020 (%)

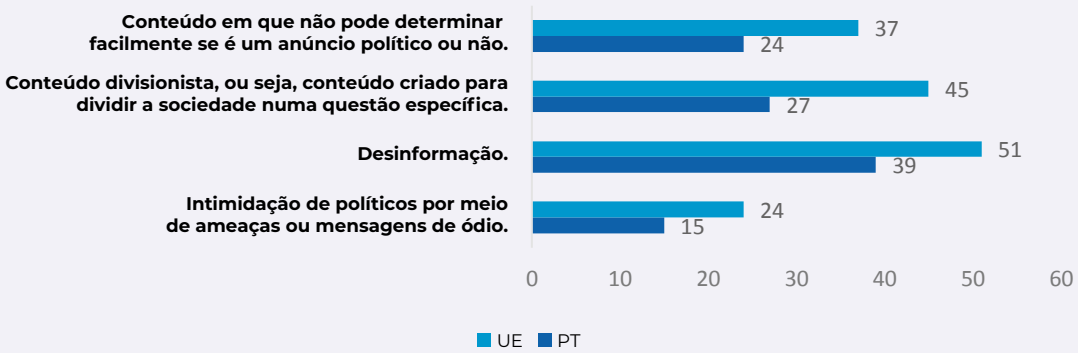


Figura 6 | Eurobarómetro, 2020

Por fim, este inquérito abordou questões próximas da cibersegurança também relativamente ao nível de exposição dos indivíduos a determinados conteúdos *online*. O tipo de conteúdo, entre os apresentados, a que os indivíduos em Portugal afirmam estar mais expostos é a desinformação, com 39%. A média da UE é bastante superior, em 12 pp, com 51%. Esta superioridade da média da UE em relação a Portugal repete-se em todas as outras situações descritas. O tipo de conteúdo a que os indivíduos se sentem menos expostos é a intimidação de políticos por meio de ameaças ou mensagens de ódio, com 15% em Portugal e 24% na média da UE.

Aspetos sociodemográficos relevantes em Portugal, 2020

Sexo **Os homens tendem a mostrar mais preocupações e a afirmarem mais estar expostos às ameaças descritas do que as mulheres.** Por exemplo, 48% dos homens afirmam ter sido expostos a desinformação *online* e apenas 30% das mulheres o fazem.

Idade **Os indivíduos com idades compreendidas entre 25 e os 54 anos tendem a reportar mais preocupação e maiores níveis de exposição a ameaças do que os indivíduos mais novos ou mais velhos.** Por exemplo, 63% dos indivíduos com idades entre os 40 e os 54 anos têm preocupações com a possibilidade de ciberataques manipularem eleições, enquanto entre as pessoas com mais de 55 anos o valor atinge os 54%.

Educação **Os indivíduos que estudaram até uma idade mais avançada tendem a ter um pouco mais de preocupações e a se sentirem mais expostos às ameaças indicadas do que os indivíduos que estudaram menos anos.** Por exemplo, 66% dos indivíduos que estudaram até depois dos 20 anos de idade estão preocupados com a possibilidade de ciberataques poderem manipular eleições, enquanto entre os indivíduos que estudaram no máximo até aos 15 anos de idade este valor atinge os 59%.

UE Valores genericamente alinhados com a média da UE, exceto relativamente à idade, visto na média da UE os indivíduos mais novos tenderem a sentirem-se mais expostos às ameaças descritas do que os restantes.

DESTAQUES

Existem mais indivíduos em Portugal em 2020 do que em 2018 preocupados com a possibilidade de as eleições serem manipuladas por meio de ciberataques, tendência contrária à da média da UE.

Esta tendência de crescimento em contraciclo com a média da UE verifica-se também quanto à possibilidade de a aplicação do voto eletrónico preocupar os indivíduos no que diz respeito a eventual fraude ou a um ciberataque.

A desinformação é o tipo de conteúdo a que os indivíduos estão mais expostos em Portugal, entre os apresentados, ainda assim abaixo da média da UE.

Os homens e os indivíduos com idades compreendidas entre os 25 e os 54 anos e aqueles que estudaram mais anos tendem a manifestar mais preocupações.

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

ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS

A Direção-Geral de Estatísticas da Educação e Ciência (DGEEC) publica anualmente os resultados de dois Inquéritos à Utilização das Tecnologias da Informação e da Comunicação a todo o universo das Câmaras Municipais, por um lado, e a todo o universo da Administração Pública Central e Regional, por outro (DGEEC, 2021a e 2021b). Estes inquéritos apresentam várias questões sobre cibersegurança, em particular desde 2019, que os relatórios sobre a componente social da cibersegurança têm acompanhado.

Através destes dados é possível monitorizar a evolução das atividades que o setor público desenvolve no sentido de uma maior ou menor proteção em relação às ameaças à sua cibersegurança. Um dos aspetos que é considerado nestes inquéritos, tratados conjuntamente neste relatório, é aquele que diz respeito ao número de entidades que definem uma estratégia para a segurança de informação.

Entidades que têm definida uma estratégia para a segurança de informação, em Portugal, 2017-2020, *Administração Pública Central e Regional e Câmaras Municipais* (%)

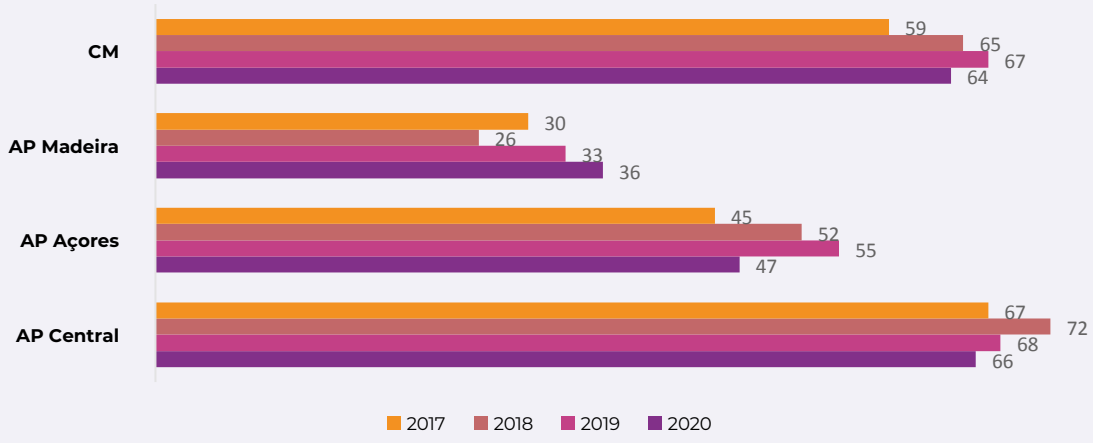


Figura 7 | DGEEC, 2021a e 2021b

Comparando com 2019, apenas a Administração Pública Regional da Madeira viu a sua percentagem de entidades com uma estratégia de segurança de informação definida aumentar, de 33% para 36%. Nos restantes organismos verificou-se um decréscimo no indicador. Por exemplo, a Administração Pública Regional dos Açores decresceu de 55% para 47%. De referir que a Administração Pública Central revela uma diminuição constante neste indicador desde 2018.

Entidades que têm definida uma estratégia para a segurança de informação, em Portugal, 2017-2020, *Conjunto da Administração Pública Central e Regional e Câmaras Municipais* (%)

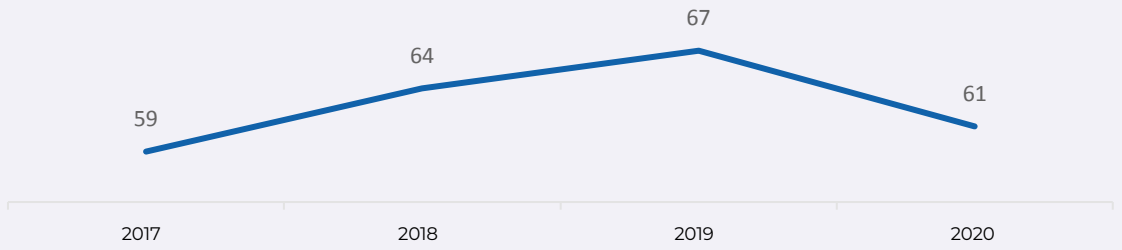


Figura 8 | DGEEC, 2021a e 2021b

Como é possível verificar pela figura 8, o ano de 2020 apresenta uma descida no conjunto de entidades da Administração Pública Central e Regional e Câmaras Municipais com uma estratégia para a segurança de informação definida, de 67% para 61%, depois de uma subida constante desde 2017.

Quanto às medidas de segurança das TIC adotadas pelas entidades da Administração Pública Central e Regional e Câmaras Municipais, é possível verificar que a atualização regular de *software* continua a ser a medida mais adotada pelas entidades. Existem ainda variações relevantes em relação ao ano anterior, nomeadamente a descida de 15 pp na adoção de técnicas de cifragem de dados na Administração Pública Regional dos Açores e o aumento de 13 pp entre as Câmaras Municipais no que diz respeito à conservação de registos para análise depois da ocorrência de incidentes de segurança.

Medidas de segurança das TIC utilizadas, em Portugal, 2019-2020, *Administração Pública Central e Regional e Câmaras Municipais* (%)

	AP Central 2020 (tendência 2019)	AP Açores 2020 (tendência 2019)	AP Madeira 2020 (tendência 2019)	CM (tendência 2019)
Atualização regular do software.	93 (-2)	100 (+2)	96 (+7)	99 (-1)
Controlo de acessos à rede do Organismo.	88 (-1)	94 (+3)	75 (-7)	92 (-1)
Autenticação dos utilizadores através de uma palavra-passe segura.	83 (-5)	98 (-2)	91 (+2)	84 (-1)
Conservação de registos para análise depois da ocorrência de incidentes de segurança.	75 (-4)	75 (=)	63 (+5)	81 (+13)
Técnicas de encriptação de dados, documentos ou e-mails.	49 (-6)	47 (-15)	48 (+1)	51 (+2)
Testes de segurança às TIC.	54 (-2)	59 (+16)	50 (+8)	50 (=)
Avaliação dos riscos ligados às TIC.	56 (-3)	47 (=)	46 (+4)	48 (+1)
Identificação e autenticação do utilizador através de métodos biométricos.	28 (+1)	41 (-2)	38 (+5)	45 (+3)

Tabela 1 | DGEEC, 2021a e 2021b

Quando questionadas sobre a necessidade de reforço de competências em TIC, as entidades da Administração Pública Central e Regional e Câmaras Municipais indicaram de forma predominante a competência em segurança como sendo de necessidade elevada, a mais indicada por todos os tipos de entidades. No caso das Câmaras Municipais, atingiu-se o valor de 78%, mais 33 pp do que no ano anterior.

Entidades que indicaram ter elevada necessidade de reforço de competências em segurança das TIC, em Portugal, 2017-2020, *Administração Pública Central e Regional e Câmaras Municipais* (%)

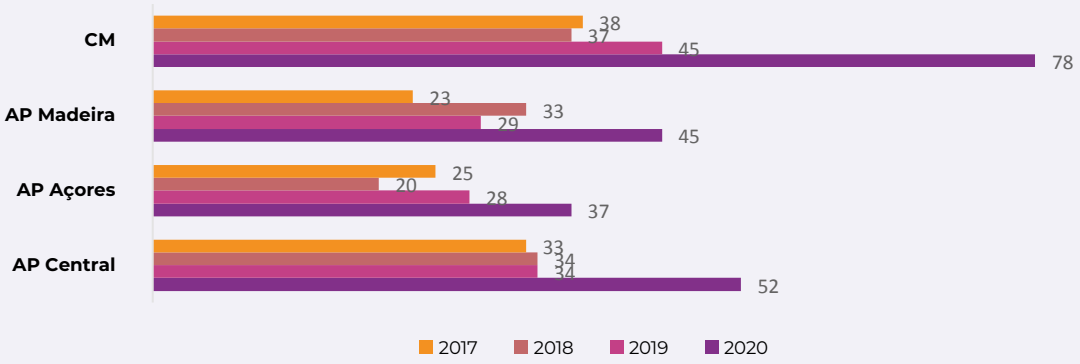


Figura 9 | DGEEC, 2021a e 2021b

No seu conjunto, passou-se de 40% para 62% de entidades da Administração Pública Central e Regional e Câmaras Municipais a indicarem a segurança como uma competência em TIC a necessitar de reforço com nível elevado, a maior subida desde 2017.

Entidades que indicaram ter elevada necessidade de reforço de competências em segurança das TIC, em Portugal, 2017-2020, *Conjunto da Administração Pública Central e Regional e Câmaras Municipais* (%)

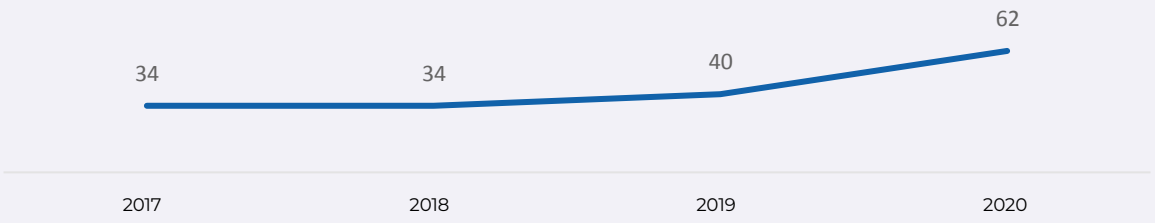


Figura 10 | DGEEC, 2021a e 2021b

No que diz respeito ao tipo de pessoal afeto a atividades relacionadas com a segurança das TIC, dados visíveis na tabela 2, o próprio organismo continua a ser a fonte principal deste pessoal. A Administração Pública Regional dos Açores lidera, com 57%, quando consideradas atividades apenas com essa fonte. Tendo em conta as atividades que têm, duplamente, alocadas pessoal de fonte própria e externa, as Câmaras Municipais atingem o valor de 96% de atividades com pessoal do próprio organismo envolvido.

Tipo de pessoal que realizou as atividades relacionadas com a segurança das TIC, em Portugal, 2019, *Administração Pública Central e Regional e Câmaras Municipais* (%)

	AP Central 2020 (tendência 2019)	AP Açores 2020 (tendência 2019)	AP Madeira 2020 (tendência 2019)	CM (tendência 2019)
Pessoal do próprio Organismo (apenas)	44 (+1)	57 (-2)	36 (-26)	42 (-2)
Fornecedores externos (apenas)	19 (+1)	22 (+1)	27 (-2)	4 (-4)
Pessoal do próprio Organismo e fornecedores externos	37 (-2)	22 (+1)	38 (+29)	54 (+7)

Tabela 2 | DGEEC, 2021a e 2021b

Outro dos aspetos relativo a atitudes e comportamentos analisados neste inquérito é o da existência ou não de recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC. Observando a figura 11, verifica-se que a Administração Pública Central é o domínio com mais entidades a referirem ter este tipo de recomendações, com 53%, mais 1 pp do que em 2019. De destacar a subida de 15 pp da Administração Pública Regional dos Açores a este respeito.

Organismos que possuem recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC, em Portugal, 2019-2020, *Administração Pública Central e Regional e Câmaras Municipais* (%)

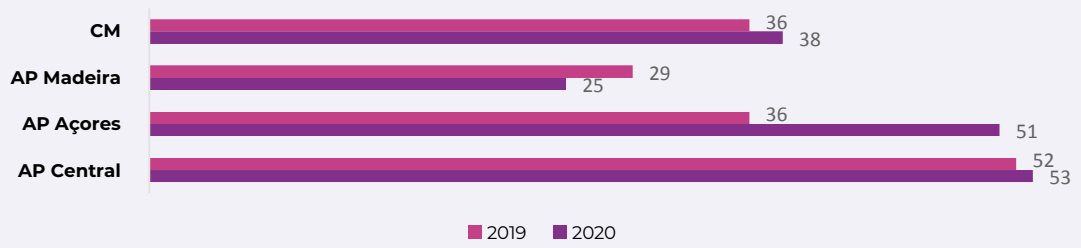


Figura 11 | DGEEC, 2021a e 2021b

Relativamente aos assuntos inscritos nas recomendações, a gestão dos níveis de acesso às TIC e o armazenamento, proteção, acesso e processamento de dados são os mais frequentemente documentados. Verifica-se ainda uma subida particularmente relevante nas recomendações sobre formação do pessoal ao serviço para uma utilização segura das TIC, com mais 23 pp entre as entidades da Administração Pública Central e na Administração Pública Regional da Madeira, mais 24 pp na dos Açores e mais 36 pp nas Câmaras Municipais – um aspeto que contribui diretamente para componentes que serão tratadas no capítulo sobre Educação e Sensibilização.

Assuntos inscritos nas recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC, em Portugal, 2019-2020, *Administração Pública Central e Regional e Câmaras Municipais* (%)

	AP Central 2020 (tendência 2019)	AP Açores 2020 (tendência 2019)	AP Madeira 2020 (tendência 2019)	CM (tendência 2019)
Gestão dos níveis de acesso às TIC.	96 (+3)	100 (+5)	93 (+1)	92 (=)
Armazenamento, proteção, acesso e processamento de dados.	94 (+1)	100 (+5)	100 (+8)	92 (+4)
Responsabilidade, direitos e deveres no que respeita à utilização das TIC.	94 (+2)	77 (-12)	100 (+23)	91 (+2)
Procedimentos ou regras para prevenir ou reagir a incidentes de segurança.	83 (+6)	77 (+9)	93 (+1)	85 (+10)
Formação do pessoal ao serviço para uma utilização segura das TIC.	91 (+23)	92 (+24)	100 (+23)	92 (+36)

Tabela 3 | DGEEC, 2021a e 2021b

No seu conjunto, na Administração Pública Central e Regional e Câmaras Municipais, passou-se de 44% em 2019 para 45% em 2020 de entidades com recomendações de algum tipo, como é visível na figura 12.

Organismos que possuem recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC, em Portugal, 2019-2020, *Conjunto da Administração Pública Central e Regional e Câmaras Municipais* (%)

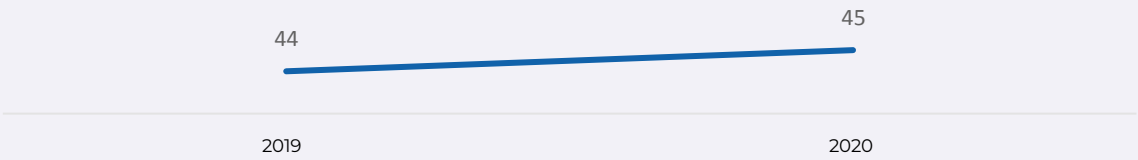


Figura 12 | DGEEC, 2021a e 2021b

OUTROS DADOS

Existem outros aspetos tratados nestes inquéritos que dizem respeito a componentes tecnológicas, incidentes e atividade económica, no âmbito da cibersegurança, analisados em diversos documentos do Observatório de Cibersegurança, que não são aprofundados neste relatório. Todavia, é relevante apresentar alguns desses indicadores de modo a compreender-se melhor o contexto em causa.

Por exemplo, na componente tecnológica da cibersegurança, o tipo de aplicação mais utilizada entre as várias organizações é o *software* antivírus, com 99% da Administração Pública Central a utilizá-lo. A menos utilizada entre as listadas, também neste tipo de organização, é o *backup* de informação numa localização externa ao Organismo, com 68%. Em ambos os casos, os valores são os mesmos do que no ano anterior. Verifica-se também um ligeiro crescimento no uso de VPN. Por exemplo, a Administração Pública Central aumentou o seu uso de 81% para 85% dos organismos.

Em termos de problemas devido a incidentes de segurança relacionados com as TIC, 16% das entidades da Administração Pública Central reconhecem ter tido algum problema deste tipo (menos 1 pp do que em 2019), enquanto apenas 6% das entidades da Administração Pública Regional dos Açores afirmam o mesmo (menos 2 pp do que em 2019). O problema mais comum entre os organismos que tiveram algum problema é a indisponibilidade de serviços TIC, devido a ataques externos, em mais de metade dos casos de todos os tipos de entidades em análise, exceto nas Câmaras Municipais, que atingem 49% dos casos.

Por fim, de referir que apenas 3% dos organismos da Administração Púbica Central possuem seguro contra incidentes de segurança das TIC, ainda assim, mais 1 pp do que em 2019. Já as Câmaras Municipais atingem os 7%, o mesmo valor do ano anterior.

Resumindo, pode dizer-se que as organizações sob análise utilizam as aplicações tecnológicas de segurança mais comuns, mas que ainda usam pouco outras igualmente importantes; o número de organismos a ter problemas resultantes de incidentes de cibersegurança mantém-se relativamente estável; e há que incrementar a utilização de seguros deste âmbito pelas entidades em causa.

Destaques

Em 2020, existem menos organismos da Administração Pública Central e Regional e Câmaras Municipais com estratégias de segurança de informação definidas do que no ano anterior.

A atualização regular do *software* é a medida de segurança das TIC mais adotada pelas entidades da Administração Pública Central e Regional e Câmaras Municipais.

A competência em TIC mais necessária para estas entidades é a relacionada com a segurança, tendo ocorrido uma subida acentuada em relação ao ano anterior.

A maioria das atividades relacionadas com a segurança da TIC nestas entidades é realizada por pessoal do próprio organismo, com as Câmaras Municipais em destaque.

Genericamente, existem mais entidades com recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC do que no ano anterior, sendo a gestão dos níveis de acesso às TIC e o armazenamento, proteção, acesso e processamento de dados os assuntos mais frequentes nessas mesmas recomendações. De destacar ainda a subida acentuada da formação do pessoal como assunto também presente.

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

Síntese - as atitudes e os comportamentos face à cibersegurança, em Portugal

Os indivíduos sabem mais do que a média da UE acerca da existência de sistemas de segurança nos *smartphones*, mas têm menos cuidados de segurança na utilização dos mesmos.

Os indivíduos aplicam o múltiplo fator de autenticação num volume ligeiramente acima da média da UE, mas, por outro lado, usam mais o *login* das redes sociais para acesso a outros serviços *online* do que a média da UE.

Embora os indivíduos manifestem ter menos conhecimento sobre a função e uso dos *cookies*, afirmam mais do que a média da UE aplicar práticas de gestão dos dados pessoais na Internet.

Existem cada vez mais indivíduos preocupados com a possibilidade de as eleições poderem ser manipuladas por meio de ciberataques, bem como quanto à eventual fraude ou ciberataque resultantes do uso do voto eletrónico. Estas tendências encontram-se em contraciclo com as tendências das médias da UE a este respeito.

O tipo de conteúdo malicioso, entre os apresentados, para a democracia a que os indivíduos estão mais expostos é a desinformação, embora menos em Portugal do que na média da UE.

As pessoas do sexo masculino, jovens e com formação superior tendem a apresentar melhores indicadores de atitudes e comportamentos face à cibersegurança do que os restantes grupos.

Existem menos entidades da Administração Pública Central e Regional e Câmaras Municipais com estratégias de segurança de informação definidas do que no ano anterior.

A competência em TIC considerada mais necessária pela Administração Pública Central e Regional e Câmaras Municipais continua a ser a que se relaciona com a segurança, de forma ainda mais acentuada do que no ano anterior.

Em média, as entidades da Administração Pública Central e Regional e Câmaras Municipais aplicam mais medidas de segurança das TIC do que no ano anterior e existem mais organismos com recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC. O assunto inscrito nessas recomendações que mais subiu foi o relativo à formação dos colaboradores.

G

SENSIBILIZAÇÃO E EDUCAÇÃO

O modo mais frequente que os governos, as organizações e os indivíduos têm para mitigar os resultados negativos de atitudes e comportamentos face à cibersegurança é através da sensibilização e educação da população. Este é um dos aspetos relativamente aos quais Portugal apresenta resultados mais positivos, se considerarmos em particular o relatório sobre a componente "Sociedade" do ano passado. O número de cursos, de ações de sensibilização e de pessoas alcançadas tem aumentado de forma consistente. Os dados deste ano mantêm a tendência do ano anterior, como será visível de seguida. Os subcapítulos que se seguem serão os seguintes: Ações de sensibilização em cibersegurança; Sensibilização na Administração Pública Central e Regional e Câmaras Municipais; Cursos de Especialização Tecnológica e Cursos do Ensino Superior; e, por fim, Alunos inscritos e diplomados no ensino superior de cibersegurança. Também relativamente aos indicadores destacados neste capítulo serão realizadas sugestões de articulação com as linhas de ação da ENSC.

AÇÕES DE SENSIBILIZAÇÃO EM CIBERSEGURANÇA

Por "sensibilização" entendem-se todas as ações que procuram consciencializar a população para os riscos do ciberespaço e as boas práticas de cibersegurança de modo a mitigar os efeitos nefastos das ameaças e das vulnerabilidades existentes. Neste âmbito, realizou-se um inquérito a algumas entidades consideradas relevantes nesta matéria em Portugal, tendo em conta sobretudo as ações sem fins lucrativos dirigidas a públicos externos às organizações. Na tabela seguinte é possível identificar o número de sessões e de cursos *online* existentes em 2020 entre as entidades consultadas que disponibilizaram dados a este respeito, entendendo-se "ações" como a agregação de sessões e cursos *online*.

Ações (sessões e cursos *online*) de sensibilização em cibersegurança realizados gratuitamente, em Portugal, 2020, *Entidades que têm como missão sensibilizar o público externo*

	Sessões de sensibilização		**Cursos *online* de sensibilização**		**Totais**	
Entidades	Sessões	Pessoas alcançadas	Cursos *online*	Pessoas alcançadas	Total de sessões e cursos	Total de pessoas alcançadas
Associação DNS.PT	5	S/D*	0	0	5	S/D
AP2SI	3	210	0	0	3	210
CNCS	52	2539	3	23312	55	25851
CIIWA	11	560	2	24	13	584
Consórcio do Centro Internet Segura (DGE, IPDJ, FCT, APAV, F. Altice, Microsoft)	2188	78837	0	0	2188	78837**
COTEC Portugal	2	700	1	1500	3	2200
IAPMEI	5	1013	1	14	6	1027
Instituto de Apoio à Criança	9	632	0	0	9	632
Polícia Judiciária	27	338	0	0	27	338
Polícia de Segurança Pública	553	8176	0	0	553	8176
TOTAL	2855	93005	7	24850	2862	117855
% por sessões, cursos e alcance	**99,76%**	**79%**	**0,028%**	**21%**	**100%**	**100%**

* S/D: sem dados.
** Alguns dados referem-se ao ano letivo 2019/2020 e não estritamente ao ano 2020.

Tabela 4 | CNCS

Nos dados apresentados é possível verificar que grande parte das ações foram realizadas através de sessões de sensibilização (99,76%), sendo num número muito menor a quantidade de cursos *online* existentes (0,028%). Contudo, em termos relativos, estes cursos têm uma capacidade de alcance muito grande, correspondendo a cerca de um quinto das pessoas alcançadas (21%), apesar de se referirem a menos de meio por cento do total de ações realizadas. De destacar que no total foram alcançadas 117 855 pessoas, distribuídas por 2 862 ações.

É importante assinalar também que a Direção-Geral da Educação (DGE) desenvolve um conjunto de iniciativas de grande alcance não integradas nesta tabela devido ao facto de abrangerem atividades curriculares de forma transversal, correspondendo por isso a uma tipologia diferente e que merece uma indicação específica. Neste âmbito incluem-se iniciativas como o Apoio às Escolas, o #Estudo em Casa, aulas de TIC e de Cidadania e Desenvolvimento, incluindo potencialmente a totalidade dos alunos e dos docentes do ensino básico. Ao nível do ensino secundário, os alunos são envolvidos em campanhas de sensibilização dinamizadas pelas próprias escolas em atividades como o Ensino a Distância (E@D), as aulas de Cidadania e Desenvolvimento, os cursos

de Informática e os projetos de sensibilização, como a Escola Sem *Bullying*, a Escola Sem Violência, Líderes Digitais e os Clubes de Informação e Comunicação[5].

No âmbito do inquérito realizado, foi possível ainda efetuar algumas questões sobre se estas entidades utilizam mecanismos de avaliação do impacto destas ações de sensibilização no comportamento dos cidadãos e, se sim, quais os métodos utilizados. O objetivo foi perceber em que medida as entidades avaliam o resultado do esforço de capacitação de modo a melhorar os conteúdos e a metodologia.

Entidades que utilizam mecanismo de avaliação do impacto das ações de sensibilização gratuitas realizadas no comportamento dos cidadãos, em Portugal, 2021, *Entidades que têm como missão sensibilizar o público externo*

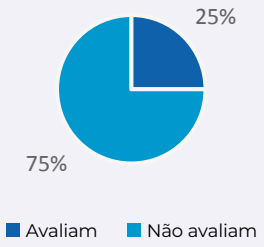


Figura 13 | CNCS

Apenas 25% das entidades afirmam realizar qualquer tipo de avaliação deste género. Destas, 75% referem que fazem observação direta ao comportamento do público-alvo, 50% fazem inquéritos e 25% dinamizam grupos de foco.

Tipo de mecanismo de avaliação do impacto das ações de sensibilização gratuitas realizadas no comportamento dos cidadãos, em Portugal, 2021, *Entidades que têm como missão sensibilizar o público externo* (%)*

* Múltiplas respostas possíveis.

Figura 14 | CNCS

5 Informação fornecida pela DGE.

Desta análise conclui-se que as entidades deverão desenvolver no futuro mais mecanismos de compreensão dos impactos da sensibilização no comportamento das pessoas alcançadas, de modo a terem uma perspetiva mais crítica e consciente sobre o seu próprio trabalho nesta matéria.

Destaques

A maioria das ações de sensibilização realizadas foram sessões presenciais ou à distância, mas os cursos *online*, em termos relativos, têm um maior poder de alcance de pessoas por cada iniciativa.

No âmbito destas ações, foram alcançadas 117 855 pessoas durante 2020.

Existe ainda um conjunto de ações com efeitos curriculares e transversais a todos os ciclos de estudos não superiores, realizados pela DGE, que alcançam, potencialmente, grande parte dos alunos e dos docentes em Portugal.

Entre as entidades inquiridas neste estudo, apenas um quarto das mesmas avalia os resultados das suas ações no comportamento dos cidadãos, sobretudo através de observação direta do público-alvo.

> Relação com as seguintes linhas de ação da ENSC: E2e, E2f, E2h, E2l e E2r (ver anexo).

SENSIBILIZAÇÃO NA ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS

Os inquéritos já apresentados realizados pela DGEEC (2021a e 2021b) à Administração Pública Central e Regional e Câmaras Municipais apresentam uma questão que permite recolher dados sobre o tipo de ação de sensibilização que as entidades da Administração Pública Central e Regional e Câmaras Municipais realizam junto do seu pessoal. Observando a tabela seguinte, verifica-se que grande parte da formação ministrada é de participação voluntária e que esta aumentou se compararmos 2019 e 2020. A Administração Pública Central destaca-se com 68% das entidades a afirmarem realizar este tipo de ação, mais 5 pp do que no ano anterior.

Tipo de ação efetuada junto do pessoal ao serviço para consciencialização das suas obrigações em matéria de segurança das TIC, em Portugal, 2019-2020, *Administração Pública Central e Regional e Câmaras Municipais* (%)

	AP Central 2020 (tendência 2019)	AP Açores 2020 (tendência 2019)	AP Madeira 2020 (tendência 2019)	CM (tendência 2019)
Ações de formação voluntária ou informação interna disponível.	68 (+5)	65 (+5)	59 (+3)	62 (+4)
Disposições contratuais.	25 (+1)	14 (+1)	9 (-2)	20 (=)
Ações de formação obrigatória e/ou consulta obrigatória de informação.	26 (+1)	16 (-3)	27 (+9)	19 (=)

Tabela 5 | DGEEC 2021a e 2021b

No seu conjunto, 65% das entidades da Administração Pública Central e Regional e Câmaras Municipais realizam ações de sensibilização voluntárias ou disponibilizam documentação aos seus colaboradores, 21% integram estas obrigações em disposições contratuais e apenas 22% têm ações com caráter obrigatório.

Tipo de ação efetuada junto do pessoal ao serviço para consciencialização das suas obrigações em matéria de segurança das TIC, em Portugal, 2020, *Conjunto das Entidades da Administração Pública Central e Regional e Câmaras Municipais* (%)

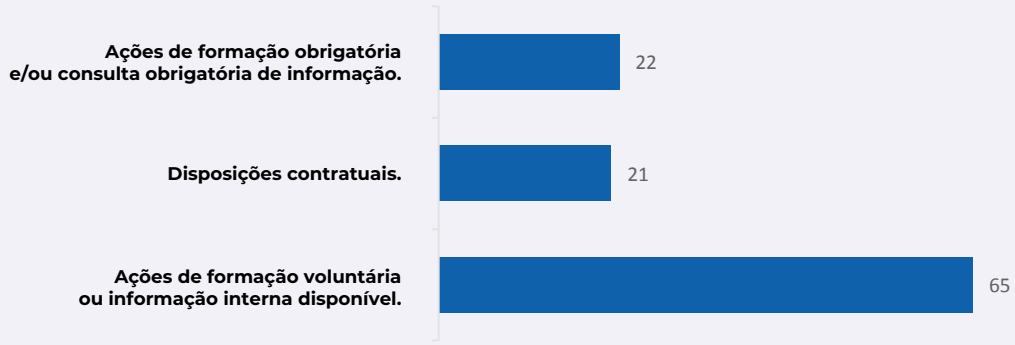


Figura 15 | DGEEC, 2021a e 2021b

DESTAQUES

O tipo de ação efetuada junto do pessoal ao serviço para consciencialização das suas obrigações em matéria de segurança das TIC maioritária, na Administração Pública Central e Regional e Câmaras Municipais, é a voluntária ou a disponibilização de informação interna.

Este tipo de ação está mais presente nestas entidades do que no ano anterior.

Relação com as seguintes linhas de ação da ENSC: E2e, E2f, E2h, E2l e E2r (ver anexo).

CURSOS DE ESPECIALIZAÇÃO TECNOLÓGICA E CURSOS DO ENSINO SUPERIOR

A componente relativa à "educação" designa neste contexto uma recolha de dados sobre os cursos dedicados à cibersegurança e segurança de informação, nomeadamente ao nível profissional, quanto a Cursos de Especialização Tecnológica (CET) e Cursos de Técnicos Superiores Profissionais (TESP), bem como no que se refere aos que atribuem um grau, isto é, licenciaturas, mestrados e doutoramentos.

Existe um aumento contínuo no número de cursos dedicados especificamente à cibersegurança e segurança de informação nos últimos anos, tendência que se mantém em 2021. Em termos de Cursos de Especialização Tecnológica, verifica-se que foi criado mais um curso de cibersegurança em 2021, depois de em 2020 terem sido lançados três. De referir que numa das instituições em que estes cursos são oferecidos, a NOVOTECNA, são disponibilizadas 9 edições deste curso em várias localidades distribuídas pelo país.

Cursos de Especialização Tecnológica de Cibersegurança e Segurança de Informação, divulgados pela DGES, em Portugal, 2021

Formação	Instituição
Cibersegurança	ATEC – Associação de Formação para a Indústria
Cibersegurança	Centro de Emprego e Formação Profissional de Coimbra
Cibersegurança (NOVO)	Centro de Emprego e Formação Profissional do Médio Tejo
Cibersegurança	Instituto Profissional de Tecnologias Avançadas para a Formação, Lda.
Cibersegurança (9 cursos)	NOVOTECNA – Associação para o Desenvolvimento Tecnológico

Tabela 6 | DGES (recolha CNCS)

No que diz respeito a cursos superiores registados pela Direção-Geral do Ensino Superior (DGES), é visível que a criação de novas formações continua a ocorrer a um ritmo anual, com mais 4 em 2021 (3 cursos TESP e 1 mestrado), como é possível verificar na tabela 7. Em 2020, tinham sido criados 2 novos cursos (1 curso TESP e 1 mestrado). A licenciatura e o doutoramento continuam a ser os tipos de graus com

menos cursos, com apenas um cada. Os cursos TESP, desde que foram concebidos, têm crescido de forma assinalável, atingindo neste momento um total de 9 cursos em cibersegurança, o mesmo volume de mestrados. No total, existem 20 cursos explicitamente de cibersegurança e segurança de informação de nível superior registados pela DGES, o que não quer dizer que não sejam formadas pessoas neste domínio noutros cursos mais genéricos da área disciplinar das TIC.

Cursos superiores de cibersegurança e segurança de informação registados pela DGES, em Portugal, 2021

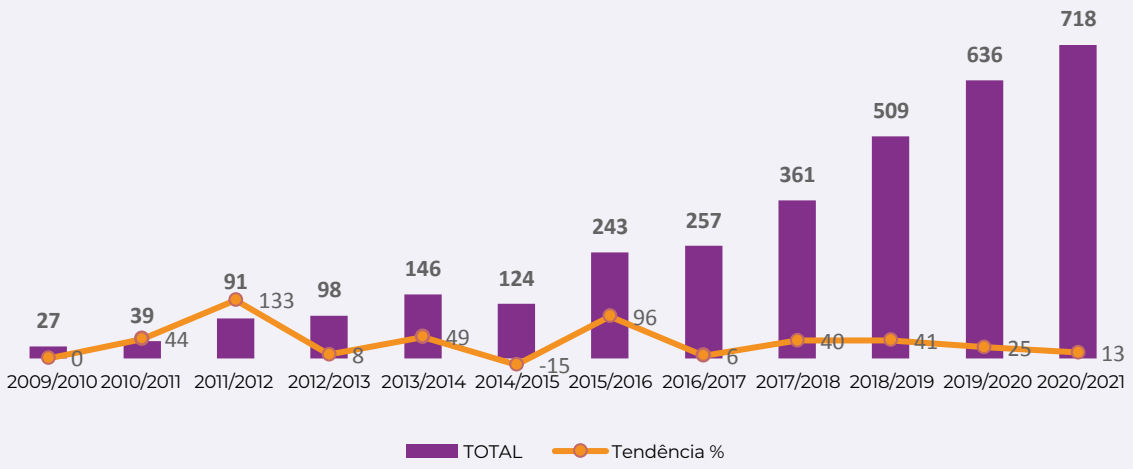
Formação	Tipo/Grau	Instituição
Cibersegurança	TESP	Instituto Politécnico da Guarda – Escola Superior de Tecnologia e Gestão
Cibersegurança	TESP	Instituto Politécnico da Lusofonia – Escola Superior de Engenharia e Tecnologias
Cibersegurança	TESP	Instituto Politécnico de Bragança – Escola Superior de Tecnologia e de Gestão de Bragança
Cibersegurança (NOVO)	TESP	Instituto Superior de Tecnologias Avançadas de Lisboa
Cibersegurança e Redes informáticas (NOVO)	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
Cibersegurança, Redes e Sistemas Informáticos	TESP	Instituto Politécnico Jean Piaget do Sul – Escola Superior de Tecnologia e Gestão Jean Piaget
Redes e Segurança Informática	TESP	Instituto Politécnico do Cávado e do Ave – Escola Técnica Superior
Segurança e Proteção de Dados para Sistemas de Informação (NOVO)	TESP	Instituto Politécnico do Cávado e do Ave – Escola Técnica Superior
Segurança Informática em Redes de Computadores	Licenciatura	Instituto Politécnico do Porto – Escola Superior de Tecnologia e Gestão
Cibersegurança	Mestrado	Instituto Politécnico de Viana do Castelo – Escola Superior de Tecnologia e Gestão
Cibersegurança	Mestrado	Universidade de Aveiro
Cibersegurança e Auditoria de Sistemas Informáticos (NOVO)	Mestrado	Instituto Superior Politécnico Gaya
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
Segurança de Informação	Doutoramento	Universidade de Lisboa – Instituto Superior Técnico

Tabela 7 | DGES (recolha CNCS)

ALUNOS INSCRITOS E DIPLOMADOS NO ENSINO SUPERIOR DE CIBERSEGURANÇA

Pelo sexto ano consecutivo, ocorre um aumento no número de alunos que se inscreveram em cursos superiores de cibersegurança e segurança de informação. Em 2020, inscreveram-se 718 alunos, uma subida de 13% em relação ao ano anterior. Esta tendência acompanha o crescimento da oferta.

Total de alunos inscritos em cursos superiores de cibersegurança e segurança de informação registados pela DGEEC e tendência, em Portugal, 2009-2021*



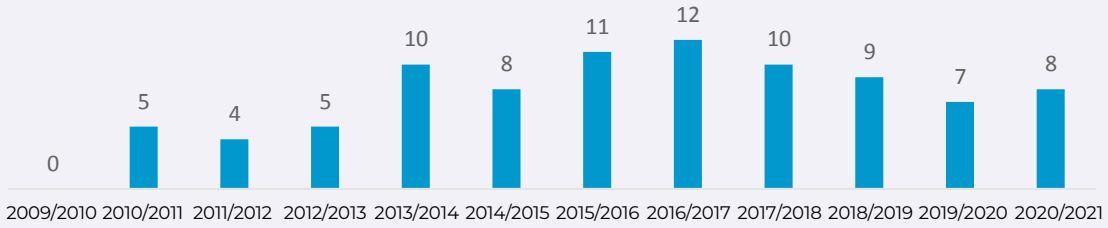
* Para efeitos de contabilização do número de alunos que se inscreveram, deixou-se de contabilizar as Pós-Graduações. Por essa razão, ocorrem ligeiros acertos relativos aos anos anteriores.

Figura 16 | DGEEC (recolha CNCS)

A percentagem de mulheres que se inscreveram nestes cursos continua a manter-se a níveis relativamente baixos, ainda que este valor tenha subido 1 pp no ano letivo 2020/2021, de 7% para 8%. Estes números revelam-se particularmente significativos se considerarmos que a percentagem de mulheres matriculadas pela primeira vez no primeiro ano em cursos de TIC em Portugal, em 2021, é de 19% (Pordata, 2021)[6].

6 https://www.pordata.pt/Subtema/Portugal/Sociedade+de+Informa%c3%a7%c3%a3o+e+Telecomunica %c3%a7%c3%b5es-92 [consultado em 06/12/2021]

Percentagem de mulheres inscritas em cursos superiores de cibersegurança e segurança de informação registados na DGEEC, em Portugal, 2009-2021 (%)*

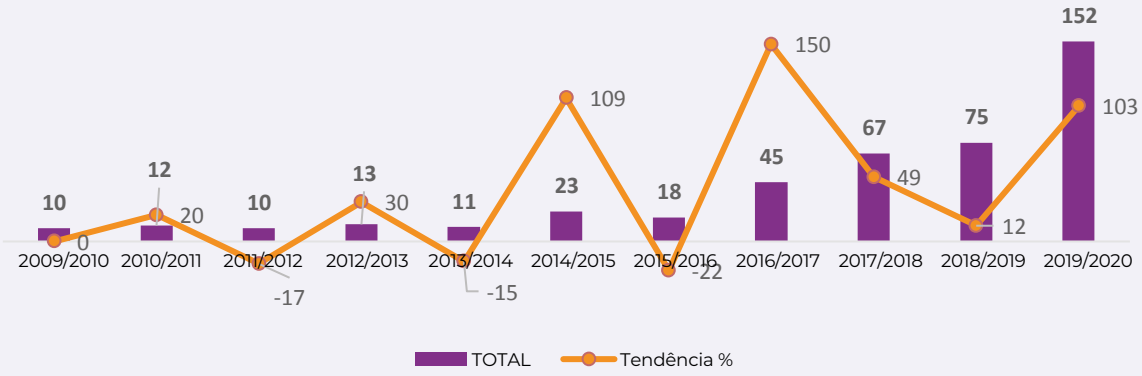


* Para efeitos de contabilização do número de alunos que se inscreveram, deixou-se de contabilizar as Pós-Graduações. Por essa razão, ocorrem ligeiros acertos relativos aos anos anteriores.

Figura 17 | DGEEC (recolha CNCS)

Quanto ao número de alunos diplomados anualmente nestes cursos, o ano letivo de 2019/2020 apresenta uma subida considerável, em 103%, de 75 para 152 alunos. A tendência de crescimento mantém-se pelo menos desde 2016. De referir que as discrepâncias entre certos anos podem estar relacionadas com a descontinuidade de alguns cursos.

Total de alunos diplomados em cursos superiores de cibersegurança e segurança de informação registados na DGEEC e tendência, em Portugal, 2009-2021*



* Para efeitos de contabilização do número de alunos que se diplomaram, deixou-se de contabilizar as Pós-Graduações. Por essa razão, ocorrem ligeiros acertos relativos aos anos anteriores.

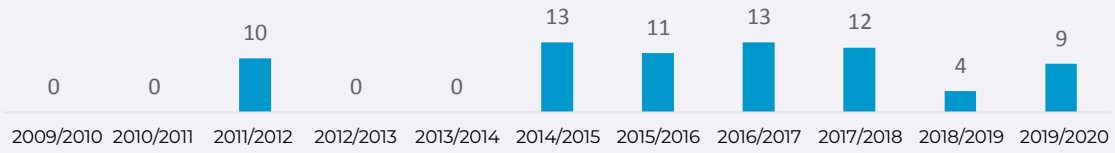
Figura 18 | DGEEC (recolha CNCS)

A percentagem de mulheres diplomadas neste tipo de cursos aumentou 5 pp no ano letivo de 2019/2020, de 4% para 9%, contrariando a tendência decrescente que se verificava desde 2016. De referir que a percentagem de mulheres diplomadas no ensino superior em cursos da área das TIC foi em 2020 de 21% (Pordata, 2021)[7]. Estes dados surgem em coerência com alguns dos resultados do estudo da AP2SI aos profissionais de cibersegurança e segurança da informação, lançado em colaboração com o Observatório de Cibersegurança, no âmbito

7 https://www.pordata.pt/Subtema/Portugal/Sociedade+de+Informa%c3%a7%c3%a3o+e+Telecomunica %c3%a7%c3%b5es-92 [consultado em 24/11/2021]

do qual apenas 14% dos respondentes são mulheres. De referir ainda que, no mesmo inquérito, 52,1% dos inquiridos afirmam possuir uma licenciatura pré-Bolonha ou mestrado e 26,7% uma licenciatura pós-Bolonha, volumes que poderão correlacionar-se com o aumento contínuo de alunos e cursos nesta área (AP2SI, 2021).

Percentagem de mulheres diplomadas em cursos superiores de cibersegurança e segurança de informação registados na DGEEC, Portugal, 2009-2020 (%)*



* Para efeitos de contabilização do número de alunos que se diplomaram, deixou-se de contabilizar as Pós-Graduações. Por essa razão, ocorrem ligeiros acertos relativos aos anos anteriores.

Figura 19 | DGEEC (recolha CNCS)

DESTAQUES

Verifica-se um aumento no número de cursos dedicados ao tema da cibersegurança e segurança de informação, em particular de cursos TESP.

Continuam a existir apenas uma licenciatura e um doutoramento explicitamente dedicados a estes temas.

O número de alunos inscritos e diplomados em cursos de cibersegurança e segurança de informação continua a aumentar de forma consistente.

A percentagem de mulheres inscritas e diplomadas nestes cursos aumentou, mas mantém-se com valores relativamente baixos se compararmos com os valores dos cursos de TIC.

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

Síntese - a sensibilização e a educação sobre cibersegurança, em Portugal

Grande parte das ações de sensibilização realizadas foram sessões presenciais ou à distância. Não obstante, os cursos *online* alcançam mais pessoas por cada curso do que as sessões de sensibilização o fazem por cada sessão.

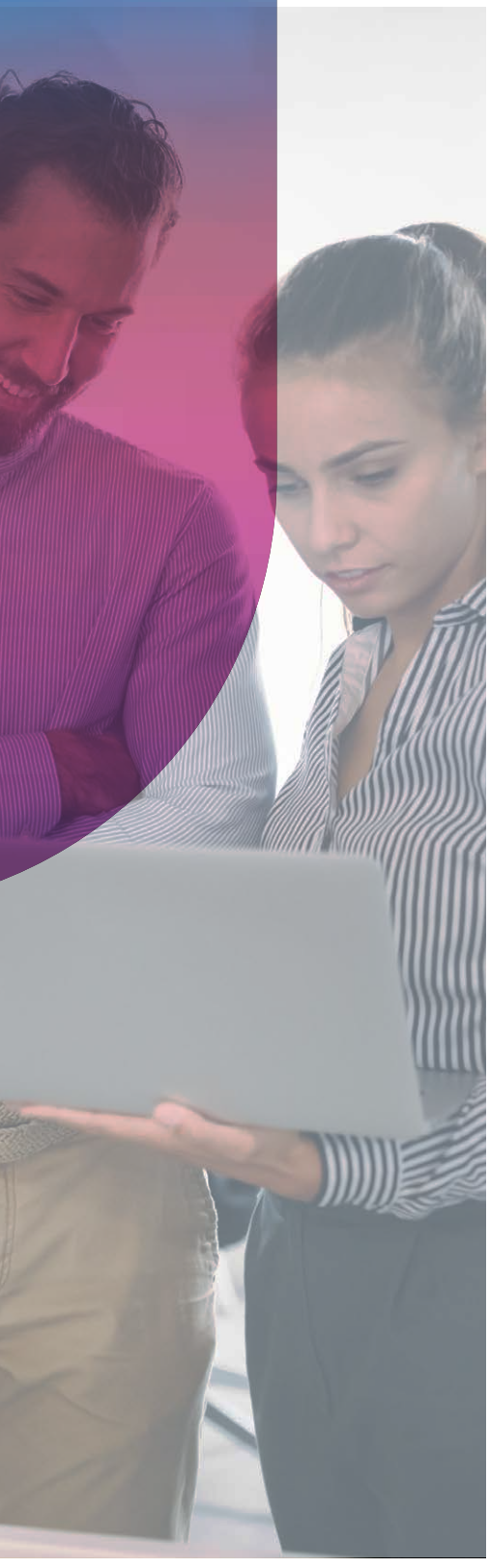
Existe um conjunto de ações de sensibilização que são integradas nas atividades curriculares e extracurriculares do ensino não superior que têm como alcance potencial todo o universo escolar em causa.

A maioria das entidades não avalia os resultados das suas ações de sensibilização no comportamento das pessoas alcançadas. Quando o fazem, utilizam maioritariamente observação direta como metodologia de análise.

As ações de sensibilização para a segurança das TIC realizadas na Administração Pública Central e Regional e Câmaras Municipais são sobretudo voluntárias.

O número de cursos dedicados ao tema da cibersegurança e da segurança de informação aumentou, em particular os cursos TESP. Não obstante, continua a existir apenas uma licenciatura e um doutoramento.

O número de alunos inscritos e diplomados nestes cursos também aumentou, mas o de mulheres mantém-se com valores relativamente baixos.



H. BRIEFING - ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO

A ENSC, aprovada pela Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, apresenta um conjunto de seis eixos de intervenção que visam capacitar o país nos vários domínios da cibersegurança. De acordo com aquele diploma, cabe ao CNCS, enquanto Autoridade Nacional de Cibersegurança, acompanhar a execução e a revisão do Plano de Ação que serve de instrumento à concretização das linhas de ação desta Estratégia, envolvendo em cooperação todas as entidades com responsabilidades nesta matéria.

É possível consultar a documentação com a análise respeitante a este tema no *website* do CNCS. O plano e os relatórios aí publicados permitem conhecer os esforços realizados pelas organizações da Administração Pública no sentido de contribuir para a boa execução da ENSC. Não obstante, pretende-se acrescentar a esta análise alguns dados que nos permitam conhecer potenciais efeitos ou impactos na sociedade das ações concretizadas. Essa é uma das missões do Observatório de Cibersegurança. Este propósito tem uma dupla dificuldade: por um lado, exige uma distância temporal razoável entre o lançamento das ações e a análise dos seus potenciais efeitos, de modo a que exista tempo suficiente para que possíveis impactos se façam sentir (daí só a partir de 2020 se considerar adequado analisar estes dados); por outro, o estabelecimento de uma correlação entre causas e efeitos neste domínio não pode ser realizada de modo direto e inequívoco, devendo-se entender este exercício mais como o colocar de hipóteses quanto a uma correlação entre variáveis (ações da estratégia e impactos na sociedade) e como a descrição de indicadores de cibersegurança que mostram a transformação positiva ou negativa da sociedade em paralelo à execução da ENSC.

É com este enquadramento em mente que se propõe articular os indicadores principais apresentados neste relatório com algumas linhas de ação da ENSC, algo que foi sendo indicado ao longo dos capítulos. Dos seis eixos de intervenção da ENSC, o eixo dois (Prevenção, Educação e Sensibilização) sobressai como aquele com o qual os dados tratados neste Relatório mais se relacionam, na medida em que é aquele eixo que mais diretamente tem potencial de impacto nas atitudes, comportamentos, sensibilização e educação. Deste eixo, por sua vez, destacam-se algumas linhas de ação em particular. Existem pelo menos nove que podem ser consideradas à luz dos dados deste relatório. No quadro do anexo é possível perceber quais são, indicando-se os aspetos mais explicitamente dirigidos às atitudes e comportamentos e aqueles que se referem à educação e sensibilização.

As linhas de ação identificadas procuram melhorar as atitudes e os comportamentos dos indivíduos face à cibersegurança, quer designando-o de forma genérica, como é o caso da linha de ação E2d, quer apelando ao desenvolvimento de formações, como é o caso da E2f, sendo que desse ponto de vista designam também, explicitamente, a sensibilização e a educação.

Observando os dados apresentados, em termos de atitudes e comportamentos, os resultados são genericamente positivos. Em termos absolutos, pouco mais de 50% dos indicadores relevados nos "destaques" ao longo deste relatório apresentam mais de metade da população em análise com dados adequados. Se compararmos com a média da UE, também aí se atinge pouco mais de 50% dos indicadores com dados acima da média. Por fim, verifica-se exatamente a mesma relação quanto à tendência, com cerca de 50% dos indicadores a este respeito com tendência de subida. Existindo ainda muito espaço de progressão nesta matéria, de quase 50%, os elementos apresentados têm fatores nos quais importa investir.

Os aspetos que exigem mais investimento em termos de conteúdos e estratégias de sensibilização são os cuidados comportamentais com os *smartphones* e o acesso a outras plataformas através do *login* das redes sociais, bem como a compreensão e gestão dos *cookies*. A relação entre democracia e cibersegurança também merece um debate mais esclarecedor. É ainda notória uma crescente necessidade de pessoal especializado em segurança das TIC na Administração Pública Central e Regional e nas Câmaras Municipais, além de uma tendência decrescente na definição de estratégias de segurança de informação nestas organizações. Estes elementos afetam transversalmente as linhas de ação da ENSC respeitantes a atitudes e comportamentos (E2d, E2e, E2f e E2h). Importa também sublinhar a persistência

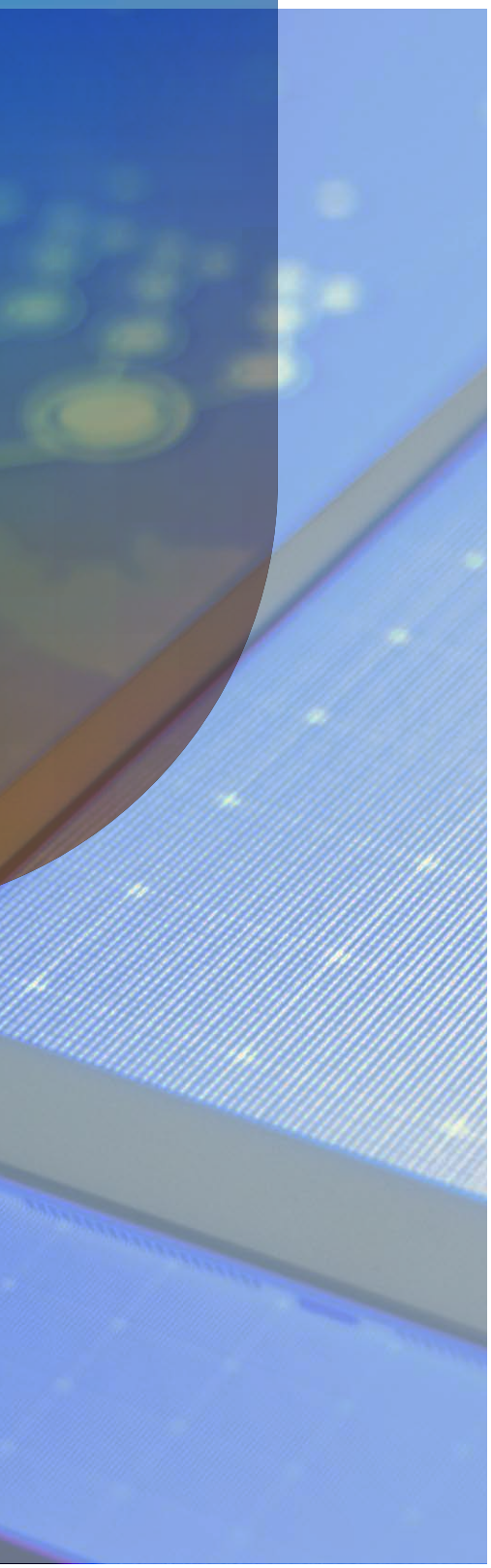
de desigualdades de género, etárias e de formação face à cibersegurança, com a constante menos positiva de mulheres, seniores e pessoas com baixa formação. Esta assimetria coloca em causa alguns elementos valorizados pelas linhas de ação E2e e E2h.

Quanto à sensibilização e educação mais concretamente, a tendência é positiva, tal como sublinhado no relatório do ano passado. Este ano, quase todos os indicadores neste domínio subiram em relação a 2019. Também é notório um esforço de capacitação no que se refere à existência de iniciativas de sensibilização, contribuindo para as linhas de ação E2e, E2f, E2h, E2l e E2r, e na criação de cursos, reforçando as linhas de ação E2g, E2k, E2l e E2m. Contudo, encontram-se algumas fragilidades, nomeadamente no número de mulheres inscritas e diplomadas, que continua a ser reduzido; quanto à avaliação das estratégias de sensibilização em termos de impacto nos comportamentos, que é muito pouco praticada; e no que diz respeito ao volume de licenciaturas e doutoramentos, que ainda é relativamente baixo.

I. RECOMENDAÇÕES

Aspetos mais críticos	Recomendações
Cuidados de segurança com os *smartphones* e o acesso a dados pessoais.	Apostar mais em conteúdos de sensibilização orientados ao uso deste dispositivo, destacando os cuidados a ter com a instalação de aplicações e o conhecimento sobre os sistemas de segurança dos *smartphones.*
Utilização do *login* das redes sociais para aceder a outros serviços *online.*	Sensibilizar as pessoas para as implicações de acederem a outros serviços *online* através do *login* das redes sociais ao nível da partilha de dados entre plataformas.
Conhecimento sobre o funcionamento dos *cookies.*	Incluir nos conteúdos de sensibilização aspetos sobre a capacidade de rastreamento dos *cookies* para uma maior consciência na navegação *online.*
Preocupação com as ciberameaças à democracia.	Promover o debate sobre esta matéria e a análise de risco que informem os indivíduos sobre o real nível de ameaça.
Exposição à desinformação.	Continuar a sensibilizar os indivíduos no sentido de saberem identificar notícias falsas e incentivar os mecanismos de mitigação da sua propagação.
Assimetrias de sexo, etárias e de formação quanto às atitudes e comportamentos.	Criar estratégias de sensibilização orientadas a grupos sociodemográficos específicos, nomeadamente seniores (tendencialmente com formação mais baixa).
Existência de menos Estratégias de Segurança de Informação na Administração Pública Central e Regional e Câmaras Municipais.	Continuar a promover, em particular no âmbito do acompanhamento da execução da ENSC, a criação de Estratégias de Segurança de Informação no setor público.
Falta de pessoal especializado em segurança das TIC na Administração Pública Central e Regional e Câmaras Municipais.	Promover a formação, a reconversão e/ou a contratação de pessoal no sentido de uma maior especialização em segurança das TIC.
Alcance das ações de sensibilização.	Promover a criação e a disseminação de MOOCs junto dos cidadãos e colaboradores das organizações públicas e privadas.
Falta de avaliação dos resultados das ações sensibilização no comportamento dos cidadãos.	Promover o estudo dos resultados das ações de sensibilização no comportamento dos públicos-alvo, aprofundando o desenvolvimento dos indicadores sobre essa matéria.
Baixa percentagem de mulheres inscritas e diplomadas nos cursos de cibersegurança e segurança de informação.	Promover as profissões ligadas à cibersegurança junto do público feminino, nas escolas e nas esferas profissionais de reconversão e habilitação profissional.
Recursos de capacitação do CNCS: 4 MOOCs (Cidadão Ciberseguro, Cidadão Ciberinformado, Consumidor Ciberseguro e Cidadão Cibersocial), Curso Geral de Cibersegurança, Curso Geral de Ciber-higiene, Centro Internet Segura, documentos de boas práticas, Recomendações Técnicas, Quadro Nacional de Referência para a Cibersegurança, Quadro de Avaliação de Capacidades de Cibersegurança, Roteiro para as Capacidades Mínimas de Cibersegurança, Webcheck, Exercício Nacional de Cibersegurança. **Consultar *website* do CNCS para aceder a estes e outros recursos** : www.cncs.gov.pt	

Quadro 1



J. NOTAS CONCLUSIVAS

A terminar 2021, foi possível compreender muito do que aconteceu em 2020 relativamente ao tema deste relatório. Se, por um lado, se verifica uma grande intensificação do uso do digital, por outro, existem alguns dados positivos quanto aos comportamentos, embora por vezes em contradição com as atitudes. Desse ponto de vista, assiste-se a uma melhoria progressiva nalguns indicadores da componente social da cibersegurança. Ainda que seja arriscado estabelecer uma correlação direta entre alguns destes resultados e possíveis causas, é importante notar que tem existido um crescente investimento na sensibilização e na educação; que em 2019 foi lançada uma nova estratégia nacional para a segurança do ciberespaço; e que, em geral, esta área começa a fazer parte dos discursos e das ações na esfera digital, com consequências relevantes a nível legislativo, político e económico. Os resultados de Portugal em índices internacionais confirmam que existe uma evolução positiva. No *Global Cybersecurity Index 2020*, da União Internacional das Telecomunicações, Portugal passou do 42º para o 14º lugar. No *National Cybersecurity Index*, desenvolvido pela e-Governance Academy Foundation, o país ocupa atualmente a 4ª posição, depois de ter estado na 14ª até há pouco tempo.

Esta constatação não deve conduzir a que se ignorem as insuficiências identificadas no presente documento, uma vez que ainda há um longo caminho a percorrer em Portugal nos vários níveis da cibersegurança. Do ponto de vista dos processos de assimilação da cibersegurança como prática comum, há que integrar este tópico na educação formal, mas também na informal, em particular na educação das crianças, como já foi referido. É preciso transmitir a literacia digital essencial para que a utilização das tecnologias digitais seja feita com o máximo cuidado desde a mais tenra idade. Atingir essa esfera

das aprendizagens em família é algo que pode demorar mais do que uma geração. Além disso, este é um processo dinâmico que exige uma constante atualização, na medida em que os riscos que o ciberespaço representa estão em permanente renovação. Neste sentido, será importante ir melhorando a produção de indicadores nesta matéria, por forma a promover as melhores estratégias de sensibilização e educação, nomeadamente estudando o grau de efetividade dos conteúdos e das técnicas utilizados.

K. NOTA METODOLÓGICA

Em termos metodológicos, o presente relatório fez uma recolha de indicadores disponíveis, realizando uma análise conjunta dos mesmos, mas também produziu indicadores através de um inquérito e de pesquisas em fontes abertas.

Os números relativos ao ambiente sociotécnico foram coletados em várias fontes que se complementaram. Os dados recolhidos em documentação da ANACOM (2021) foram produzidos com base em inquérito realizado por esta entidade junto dos prestadores de comunicações eletrónicas. Os valores publicados pelo INE resultam de dois inquéritos: o *Inquérito à Utilização de Tecnologias da Informação e da Comunicação pelas Famílias – 2020* (INE, 2020a), com frequência anual, que decorreu entre abril e agosto de 2020, e utilizou uma amostra representativa de 5094 agregados familiares domésticos residentes em Portugal, em que pelo menos um indivíduo tinha uma idade compreendida entre os 16 aos 74 anos; e o *Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Empresas – 2020* (INE, 2020b), também anual, aplicado entre março e junho de 2020, obtendo 3224 respostas válidas de uma população constituída por empresas não financeiras, com 10 ou mais pessoas ao serviço e residência em Portugal. Em complemento aos números do INE, consultaram-se as versões do Eurostat, de nível europeu: *Individuals – internet use* (Eurostat, 2020a) e *Individuals – internet activities* (Eurostat, 2020b). Sobre o confinamento social, os indicadores foram produzidos pelo INE (2021) e pelo GEE-METD (2021) através de informação disponibiliza por diversas plataformas digitais. Os dados diários foram convertidos em dados mensais.

O capítulo sobre as atitudes e os comportamentos recorreu aos seguintes inquéritos do Eurostat: T*rust, security and privacy – smartphones (2020 onwards)* (Eurostat, 2020d), *Identification procedures used for online services (2020 onwards)* (Eurostat, 2020e) e *Privacy and protection of personal data (2020 onwards)* (Eurostat, 2020f), qualquer deles realizado em Portugal pelo INE no âmbito do *Inquérito à Utilização de Tecnologias da Informação e da Comunicação pelas Famílias – 2020* (INE, 2020a), já referido, e, portanto, nas condições descritas. Também contribuiu para este capítulo o Eurobarómetro Especial 507 (Eurobarómetro, 2020), sobre a Democracia na UE, no âmbito do qual foram feitas 1007 en-

trevistas a pessoas com mais de 15 anos, em Portugal, entre outubro e novembro de 2020, pela *Marktest – Marketing, Organização e Formação*. Por fim, os dados da DGEEC resultam dos inquéritos aplicados por esta entidade: o *Inquérito à Utilização de Tecnologias da Informação e da Comunicação na Administração Pública Central e Regional*, realizado entre outubro de 2020 e fevereiro de 2021 (DGEEC, 2021a), e o *Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Câmaras Municipais*, que decorreu entre outubro de 2020 e março de 2021 (DGEEC, 2021b). Ambos os inquéritos são dirigidos a todo o universo em causa e são de resposta obrigatória. Deve sublinhar-se que o inquérito à Administração Pública, no que à Administração Central diz respeito, refere-se a organismos com esta categoria (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.

Por fim, o capítulo dedicado à sensibilização e educação resulta em parte de uma recolha, seleção e análise de dados realizada pelo CNCS em fontes abertas através do uso de palavras-chave, nomeadamente da DGEEC e da DGES, como é o caso dos que se referem a cursos e alunos inscritos e diplomados. Neste aspeto, o CNCS beneficiou da colaboração de uma equipa do Centro de Investigação e Intervenção Educativas da Universidade do Porto. Os valores sobre as ações de sensibilização na Administração Pública Central e Regional e Câmaras Municipais foram resultado dos inquéritos da DGEEC já mencionados. Aplicou-se ainda um questionário a um conjunto de organizações consideradas relevantes segundo os critérios da notoriedade, da relação com o CNCS e da realização de ações sem fins lucrativos de sensibilização em cibersegurança, para públicos externos à entidade. O questionário foi disponibilizado entre os dias 18 e 31 de outubro de 2021, através de plataforma *online*, a 39 entidades, obtendo-se 16 respostas válidas.

Para informações mais detalhadas sobre as fontes pesquisadas e as metodologias utilizadas pelas mesmas, consultar referências principais e/ou contactar o CNCS.

L. ENTIDADES PARCEIRAS DO ÂMBITO DA LINHA DE OBSERVAÇÃO SOCIEDADE

AP2SI - Associação Portuguesa para a Promoção da Segurança da Informação

APAV - Associação Portuguesa de Apoio à Vítima

Associação DNS.PT

CIIWA - Competitive Intelligence and Information Warfare Association

Consórcio Centro Internet Segura

COTEC Portugal - Associação Empresarial para a Inovação

DGE - Direção-Geral da Educação

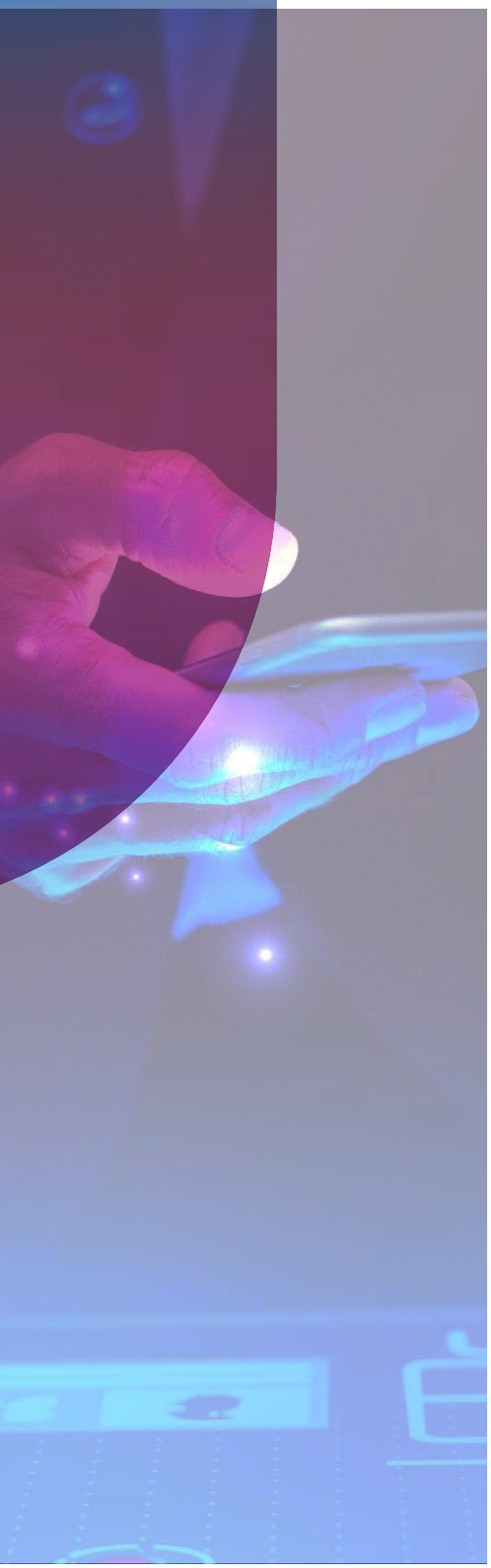
DGEEC - Direção-Geral de Estatísticas da Educação e Ciência

IAPMEI - Agência para a Competitividade e Inovação

Instituto de Apoio à Criança

IPDJ - Instituto Português do Desporto e Juventude

Polícia Judiciária



M. 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/

N. 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)

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)

***Deep fake*:** "falsificações profundas, vídeos falsos realizados com recurso à inteligência artificial e à aprendizagem automática."

(TCE, 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 nº 46/2018)

Phishing: "mecanismo de elaboração de mensagens que usam técnicas de engenharia social de modo a 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."

(ENISA, 2019)

Ransomware: tipo de *software* malicioso que permite que "um atacante se apodere dos ficheiros e/ou dispositivos de uma vítima, bloqueando a possibilidade de esta poder aceder-lhes. Para a recuperação dos ficheiros, é exigido ao proprietário um resgate em criptomoedas."

(ENISA, 2019)

ANACOM: Autoridade Nacional de Comunicações.

AP Açores: Administração Pública Regional dos Açores.

APAV: Associação Portuguesa de Apoio à Vítima.

AP Central: Administração Pública Central.

AP Madeira: Administração Pública Regional da Madeira.

AP2SI: Associação Portuguesa para a Promoção da Segurança da Informação.

CERT.PT: Equipa de Resposta a Incidentes de Segurança Informática Nacional (Lei nº 46/2018) [CERT – Computer Emergency Response Team].

CET: Curso de Especialização Tecnológica.

CIIWA: Competitive Intelligence and Information Warfare Association.

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.

ENSC: Estratégia Nacional de Segurança do Ciberespaço 2019-2023.

FCT: Fundação para a Ciência e Tecnologia.

IAPMEI: Agência para a Competitividade e Inovação.

INE: Instituto Nacional de Estatística.

IPDJ: Instituto Português do Desporto e Juventude.

MOOC: Curso Online Aberto e Massivo [Massive Open Online Course]

Pp: pontos percentuais.

PT: Portugal.

QNRCS: Quadro Nacional de Referência para a Cibersegurança.

TESP: Curso Técnico Superior Profissional.

TIC: Tecnologias de Informação e Comunicação.

UE: União Europeia.

0. REFERÊNCIAS PRINCIPAIS

RELATÓRIOS [consultados a 06/12/2021]:

ANACOM (2021) *Pandemia Covid-19: Impacto na utilização dos serviços de comunicações*. Autoridade Nacional de Comunicações. Disponível em: https://www.anacom.pt/render.jsp?contentId=1603793

CNCS (2019) *Relatório Cibersegurança em Portugal – Sociedade 2019*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/relatrio-sociedade-2019-observatrio-de-ciberseguranа-cncs-v3-1.pdf

CNCS (2020) *Relatório Cibersegurança em Portugal – Sociedade 2020*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/relatorio-sociedade2020-observatoriocibersegurancа-cncs-1.pdf

CNCS (2021) *Relatório Cibersegurança em Portugal – Riscos & Conflitos 2021*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurancа-cncs.pdf

INE (2021) *Indicadores de contexto demográfico e da expressão territorial da pandemia COVID-19 em Portugal*. Instituto Nacional de Estatística. Disponível em: https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=494189896&att_display=n&att_download=y

ITU (2021) *Global Cybersecurity Index 2020*. International Telecommunication Union. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Silva, P.A., Carmo, R.M., Cantante, F., Cruz, C.M., Estêvão, P., Manso, L., Pereira, T.S., Lamelas, F. (2020). *Trabalho e desigualdades no Grande Confinamento (II). Desemprego, layoff e adaptação ao teletrabalho*. Estudos CoLABOR, N.º2. CoLABOR. Disponível em: https://colabor.pt/publicacoes/trabalho-desigualdades-grande-confinamento-ii-desemprego-layoff-teletrabalho/

INQUÉRITOS [consultados a 06/12/2021]:

AP2SI (2021) *Estudo sobre os profissionais de cibersegurança e segurança da informação em Portugal (2021)*. Associação Portuguesa para a Promoção da Segurança da Informação. Disponível em: https://ap2si.org/iniciativas-ap2si/inquerito/resultados-2021/

DGEEC (2021a) *Inquérito à Utilização das Tecnologias da Informação e Comunicação na Administração Pública Central e Regional – IUTICAP 2020*. Direção-Geral de Estatísticas da Educação e Ciência. Disponível em: https://www.dgeec.mec.pt/np4/12.html

DGEEC (2021b) *Inquérito à Utilização das Tecnologias da Informação e Comunicação nas Câmaras Municipais- IUTICCM 2020*. Direção-Geral de Estatísticas da Educação e Ciência. Disponível em: https://www.dgeec.mec.pt/np4/12.html

Eurobarómetro (2020) *Special Eurobarometer 507: Democracy in the EU*. Eurobarómetro. Disponível em: https://data.europa.eu/data/datasets/s2263_94_1_507_eng?locale=en

Eurostat (2020a) *Individuals – internet use*. Eurostat. ISOC_CI_IFP_IU. Disponível em: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_ci_ifp_iu

Eurostat (2020b) *Individuals – internet activities*. Eurostat. ISOC_CI_AC_I. Disponível em: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_ci_ac_i

Eurostat (2020c) *Internet purchases by individuals (2020 onwards)*. Eurostat. ISOC_EC_IB20. Disponível em: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_ec_ib20

Eurostat (2020d) *Trust, security, and privacy – smartphones (2020 onwards)*. Eurostat. ISOC_CISCI_SP20. Disponível em: https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cisci_sp20&lang=en

Eurostat (2020e) *Identification procedures used for online services*. Eurostat. ISOC_CISCI_IP20. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_ip20/default/table?lang=en

Eurostat (2020f) *Privacy and protection of personal data (2020 onwards)*. Eurostat. ISOC_CISCI_PRV20. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_PRV20__custom_524270/bookmark/table?lang=en&bookmarkId=b1319f95-fcf5-4a46-8cab-b54267cce281

GEE-METD (2021) *Indicadores de Conjuntura Covid-19*. Gabinete de Estratégias e Estudos do Ministério da Economia e Transição Digital. Disponível em: https://www.gee.gov.pt/pt/indicadores-diarios/ultimos-indicadores/31496-indicadores-de-conjuntura-covid-101

INE (2020a) *Inquérito à Utilização de Tecnologias da Informação e da Comunicação pelas Famílias – 2020*. Instituto Nacional de Estatística. Disponível em: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=415621509&DESTAQUESmodo=2&xlang=pt

INE (2020b) *Inquérito á Utilização de Tecnologias da Informação e da Comunicação nas Empresas – 2020*. Instituto Nacional de Estatística. Disponível em: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=415622957&DESTAQUESmodo=2&xlang=pt

OUTROS DOCUMENTOS [consultados a 06/12/2021]:

EC (2021) *Índice de Digitalidade da Economia e da Sociedade (IDES) de 2021 – Portugal*. Comissão Europeia. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/desi-portugal

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

ENISA (2019) *ENISA Threat Landscape Report 2018*. ENISA-European Union Agency for Cybersecurity. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

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

TCE (2019) *Desafios à Eficácia da Política de Cibersegurança da UE, Tribunal de Contas Europeu*. Disponível em: https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_pt.pdf

LEGISLAÇÃO (consultada a 06/12/2021)

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

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 06/12/2021]:

www.cncs.gov.pt

www.dgeec.mec.pt

www.pordata.pt

www.ncsi.ega.ee/

N. ANEXO – LINHAS DE AÇÃO DA ENSC - SOCIEDADE

Linhas de Ação da ENSC, 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.		
Esk)	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 (E2) e na sequência pela qual surgem as linhas de ação, alinhadas com a ordem alfabética.

Quadro 2

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

Observatório
de **Cibersegurança**