CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

RELATÓRIO

CIBERSEGURANÇA EM PORTUGAL

Sociedade 2020

DEZEMBRO DE 2020

Observatório
de **Cibersegurança**

ÍNDICE

Observatório de Cibersegurança

A. SUMÁRIO EXECUTIVO

O *Relatório Cibersegurança em Portugal – Sociedade 2020* apresenta indicadores atualizados, nomeadamente de 2019, sobre o estado das atitudes, dos comportamentos e da educação e sensibilização, em Portugal, no que diz respeito à cibersegurança. O Relatório incide na componente humana deste domínio, tendo em conta os indivíduos e as organizações.

Considerando os números absolutos, a comparação com a média da União Europeia (UE) e a tendência em relação ao ano anterior, é possível extrair algumas conclusões sobre esta matéria. Verifica-se que os indivíduos e as organizações, em Portugal, não têm ainda o nível de atitudes e comportamentos suficientemente adequados para a melhor proteção possível contra as ameaças do ciberespaço, comparativamente à média da UE. Não obstante, os dados absolutos e as tendências anuais são, em parte, positivos. A componente educacional e de sensibilização tem vindo a ganhar robustez, apresentando indicadores também mais favoráveis. Em suma, à luz da metodologia adotada numa síntese dos indicadores, o resultado global, ainda que insuficiente, encontra-se junto ao limite do positivo.

Analisando os dados diretamente relacionados com as ciberameaças identificadas no *Relatório Cibersegurança em Portugal - Riscos & Conflitos 2020* (CNCS, 2020a), como o *phishing* e o *software* malicioso, é notório que os indivíduos no país tendem a manifestar preocupação com estas ameaças, contudo, não possuem ainda os comportamentos preventivos suficientes.

Tendo em conta que os indicadores mais atualizados se referem ao ano de 2019, não é possível identificar consequências da pandemia de Covid-19 nos números estudados. Todavia, os resultados mostram qual o nível de preparação dos indivíduos e das organizações para as ciberameaças que acompanham a pandemia. É reconhecido que a engenharia social é muito

importante entre as estratégias de ataque a pessoas isoladas em trabalho à distância. O *phishing*, por exemplo, aumentou, segundo dados internacionais e do CERT.PT (CNCS, 2020a, 2020b, 2020c e 2020d), o que mostra que as insuficiências comportamentais da prevenção quanto a esta ameaça podem indiciar menos preparação das pessoas e maior necessidade de formação. Quanto às compras *online*, hábito impulsionado pelo confinamento, os indivíduos em Portugal evidenciam atitudes e comportamentos mais adequados em termos de cibersegurança.

Considera-se que as conclusões deste Relatório podem ajudar a melhorar os conteúdos e as estratégias de educação e sensibilização em matéria de cibersegurança, quer nos âmbitos da educação formal e informal, quer no que diz respeito à operacionalização da componente formativa do Quadro Nacional de Referência para a Cibersegurança (QNRCS) e do Roteiro para Capacidades Mínimas de Cibersegurança (RCMCS) (CNCS, 2019b e 2019c).

B. — DESTAQUES[1]

1 Para um maior detalhe quanto ao universo considerado em cada indicador, consultar o restante relatório e o desenvolvimento de cada um dos indicadores.

ATITUDES

Preocupações dos indivíduos em relação ao uso da Internet para atividades como o banco *online* ou a compra de bens e serviços *online*, em 2019 (Eurobarómetro 499).

74% **EM PORTUGAL**
(-4 pp do que no ano anterior);

79% **NA MÉDIA DA UE**
quanto ao total de pessoas com alguma preocupação.

Preocupação dos indivíduos com o uso indevido de dados pessoais em atividades como o banco *online* ou a compra de bens e serviços *online*, em 2019 (Eurobarómetro 499).

54% **EM PORTUGAL**
(+5 pp do que no ano anterior);

46% **NA MÉDIA DA UE**
com esta preocupação.

Medo dos indivíduos de não receberem produtos ou serviços comprados *online*, em 2019 (Eurobarómetro 499).

20% **EM PORTUGAL**
(-15 pp do que no ano anterior);

22% **NA MÉDIA DA UE**
com esta preocupação.

Informação dos indivíduos sobre os riscos de cibercrime, em 2019 (Eurobarómetro 499).

2% **EM PORTUGAL**
(-1 pp do que no ano anterior);

11% **NA MÉDIA DA UE**
a sentirem-se muito bem informados.

Perfil do indivíduo, em Portugal, a sentir-se bem informado, em 2019 (Eurobarómetro 499).

+ **FREQUENTE ENTRE HOMENS, JOVENS E PESSOAS COM MAIS ESTUDOS.**

ATITUDES

Perceção dos indivíduos sobre a capacidade de se protegerem contra o cibercrime, em 2019 (Eurobarómetro 499).

45% **EM PORTUGAL**
(-8 pp do que no ano anterior);

52% **NA MÉDIA DA UE**
(-9 pp do que no ano anterior)
a sentirem-se capazes de se proteger.

Preocupação dos indivíduos com a possibilidade de serem vítimas de cibercrime, em 2019 (Eurobarómetro 499).

Crescimento generalizado.
Por exemplo:

77% **EM PORTUGAL**
(+9 pp do que no ano anterior);

66% **NA MÉDIA DA UE**
(-4 pp do que no ano anterior)
estão preocupados com o roubo de identidade.

Conhecimento, por parte dos indivíduos, de pessoas que foram vítimas de cibercrime, em 2019 (Eurobarómetro 499).

16% **EM PORTUGAL**
(-9 pp do que no ano anterior);

46% **NA MÉDIA DA UE**
(-4 pp do que no ano anterior)
conhecem alguém vítima de cibercrime.

Conhecimento dos indivíduos sobre o meio através do qual reportar um cibercrime ou qualquer outro comportamento ilegal *online*, em 2019 (Eurobarómetro 499).

18% **EM PORTUGAL**

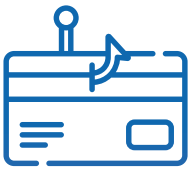
22% **NA MÉDIA DA UE**
têm consciência de um meio deste tipo.

O que fariam os indivíduos em caso de serem vítimas de alguma ciberameaça, em 2019 (Eurobarómetro 499).

CONTACTAVAM A POLÍCIA, EM TODAS AS SITUAÇÕES, EM PORTUGAL E NA MÉDIA DA UE.

Comportamentos Individuais

Alteração de comportamento dos indivíduos em resultado de preocupação com a Internet, em 2019 (Eurobarómetro 499).



Por exemplo:

43% **EM PORTUGAL**

42% **NA MÉDIA DA UE**

não abrem *emails* de pessoas desconhecidas.

No total, há mais alterações de comportamento em Portugal do que no ano anterior (+4 pp).

Alterações de comportamento dos indivíduos que mais subiram e diminuíram em resultado de preocupação com a Internet, em 2019 (Eurobarómetro 499).

20% **EM PORTUGAL**

(+7 pp do no ano anterior);

usaram *passwords* diferentes para diferentes *websites*;

35% **EM PORTUGAL**

(-9 pp do que no ano anterior)

instalaram *software* antivírus.

Alteração de *password* dos indivíduos nos 12 meses anteriores ao inquérito, em 2019 (Eurobarómetro 499).

41% **EM PORTUGAL**

(+1 pp do que no ano anterior);

69% **NA MÉDIA DA UE**

(+11 pp do que ano anterior)

mudaram pelo menos uma *password*.

Experiência dos indivíduos como vítimas de cibercrime, em 2019 (Eurobarómetro 499).

Portugal sempre abaixo da média da UE.

Por exemplo:

11% **EM PORTUGAL**

(-13 pp do que no ano anterior);

28% **NA MÉDIA DA UE**

descobriram *software* malicioso.

(receber *emails* fraudulentos ou telefonemas a pedir os seus dados pessoais é a experiência mais frequente na UE, com 36%; em Portugal representa apenas 5%)

O que fizeram os indivíduos quando foram vítimas de alguma ciberameaça, em 2019 (Eurobarómetro 499).

NÃO CONTACTARAM A POLÍCIA, NA MAIORIA DAS SITUAÇÕES, EM PORTUGAL.

Ao contrário, aqueles que imaginaram o que fariam caso fossem vítimas, respondem que contactavam a polícia.

Todavia, frequentemente, os indivíduos, em Portugal, agem mais do que a média da UE.

Comportamentos Individuais

Reporte de cibercrime ou outro comportamento ilegal *online* alguma vez feito por parte dos indivíduos, em 2019 (Eurobarómetro 499).

4% **EM PORTUGAL**

17% **NA MÉDIA DA UE**
já reportaram.

O que fazem os indivíduos em relação ao assédio *online* de crianças, em 2019 (Eurobarómetro 499).

26% **EM PORTUGAL**
(-3 pp do que no ano anterior);

37% **NA MÉDIA DA UE**
fazem algo.
(Apenas 12% discutem os riscos *online* com os filhos, mais 1 pp do que no ano anterior, contra 20% da média da UE).

Indivíduos que não compram/encomendam bens ou serviços pela Internet para uso privado, devido a preocupações com a segurança de pagamento, em 2019 (Eurostat, 2020a).

23% **EM PORTUGAL**

6% **NA MÉDIA DA UE**
não compraram/encomendaram *online* devido à segurança de pagamento.

Cópias de segurança realizadas pelos indivíduos, em 2019 (Eurostat, 2020b).

39% **EM PORTUGAL**

48% **NA MÉDIA DA UE**
fazem cópias de segurança.

Comportamentos Organizacionais

Medidas de segurança das TIC utilizadas pelas empresas, em 2019 (Eurostat, 2020c).

98% EM PORTUGAL

93% NA MÉDIA DA UE
aplicam alguma medida de segurança das TIC.

Políticas de segurança das TIC nas empresas, em 2019 (Eurostat, 2020c).

28% EM PORTUGAL

34% NA MÉDIA DA UE
têm políticas de segurança das TIC definidas.

Empresas que possuem recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC, em 2019 (Eurostat, 2020c).

28% EM PORTUGAL

34% NA MÉDIA DA UE
possuem recomendações documentadas.

Realização das atividades relacionadas com a segurança das TIC nas empresas, em 2019 (Eurostat, 2020c).

75% EM PORTUGAL

63% NA MÉDIA DA UE
recorrem a fornecedores externos para estas atividades.

Entidades Públicas, em Portugal, com uma Estratégia para a Segurança da Informação definida, em 2019 (DGEEC, 2020a e 2020b).

68% DA ADMINISTRAÇÃO PÚBLICA CENTRAL
(-4 pp do que no ano anterior);

67% DAS CÂMARAS MUNICIPAIS
(+2 pp do que ano anterior)
possuem uma estratégia.

Necessidade de reforço de competências TIC ligadas à segurança das Entidades Públicas, em Portugal, em 2019 (DGEEC, 2020a e 2020b).

45% DAS CÂMARAS MUNICIPAIS
(+8 pp do que ano anterior)
classificam esta necessidade com um grau elevado.

Medidas de segurança das TIC utilizadas pelas Entidades Públicas, em Portugal, em 2019 (DGEEC, 2020a e 2020b).

59% DA ADMINISTRAÇÃO PÚBLICA CENTRAL
faz avaliação de riscos ligados às TIC.

Tipo de pessoal que realizou as atividades relacionadas com a segurança das TIC, nas Entidades Públicas, em Portugal, em 2019 (DGEEC, 2020a e 2020b).

43% DA ADMINISTRAÇÃO PÚBLICA CENTRAL
recorreu apenas a pessoal do próprio organismo;

39% recorreu apenas a fornecedores externos.

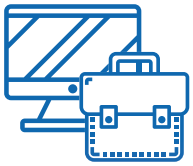
Entidades Públicas, em Portugal, que possuem recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC, em 2019 (DGEEC, 2020a e 2020b).

29% DA ADMINISTRAÇÃO PÚBLICA REGIONAL DA MADEIRA

36% DA ADMINISTRAÇÃO PÚBLICA REGIONAL DOS AÇORES
possuem recomendações documentadas.

Educação e Sensibilização

Cursos profissionais de Cibersegurança, em Portugal, em 2020. (DGES)



4 **CURSOS DE ESPECIALIZAÇÃO TECNOLÓGICA EM CIBERSEGURANÇA**
(+3 do que em 2018).

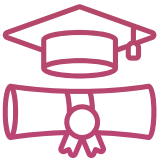
Cursos superiores de Cibersegurança e Segurança da Informação, em Portugal, em 2020 (DGES).

6 **CURSOS TÉCNICOS SUPERIORES PROFISSIONAIS**
1 **LICENCIATURA**
8 **MESTRADOS**
1 **DOUTORAMENTO**
(+1 TESP e +1 Mestrado do que em 2019).

Número de alunos que se inscreveram em cursos superiores de Cibersegurança e Segurança de Informação, em Portugal, no ano 2019/2020 (DGEEC).

636 **ALUNOS QUE SE INSCREVERAM**
(+25% do que no ano letivo anterior);
10% **MULHERES**
(-1 pp do que no ano letivo anterior).

Número de alunos diplomados em cursos superiores de Cibersegurança e Segurança de Informação, em Portugal, no ano 2018/2019 (DGEEC).



75 **ALUNOS DIPLOMADOS**
(-15% do que no ano letivo anterior);
4% **MULHERES**
(-11 pp do que no ano letivo anterior).

Número de pessoas alcançadas pelos programas de sensibilização em cibersegurança e segurança da informação, em 2019 (CCIS).

421 488
PESSOAS ALCANÇADAS
nas celebrações do Dia da Internet Mais Segura, pelo Consórcio Centro Internet Segura.

Sensibilização dos colaboradores sobre a segurança das TIC nas empresas, em 2019 (Eurostat, 2020c).

54% **EM PORTUGAL**
62% **NA MÉDIA DA UE**
tornam os colaboradores conscientes das suas obrigações.

Tipo de ação efetuada, pelas Entidades Públicas, junto do pessoal ao serviço, para consciencialização das suas obrigações em matéria de segurança das TIC, em 2019 (DGEEC, 2020a e 2020b).

63% **DA ADMINISTRAÇÃO PÚBLICA CENTRAL**
realiza ações de formação voluntárias;
25% realiza ações de formação obrigatória.

C. INTRODUÇÃO

A cibersegurança e a sociedade voltam a encontrar-se neste *Relatório Cibersegurança em Portugal - Sociedade 2020*. O texto deste ano procura avaliar a evolução de grande parte dos indicadores já apresentados no ano anterior, agora com incidência em 2019, mas também acrescentar indicadores entretanto surgidos ou atualizados, que complementam uma informação que se quer panorâmica sobre a cibersegurança em Portugal no âmbito em apreço.

Tal como o documento de 2019, o de 2020 divide-se em três temas centrais: as atitudes; os comportamentos; e a educação e sensibilização. Fruto do lançamento dos resultados de três inquéritos importantes (um do Eurostat, sobre as Empresas, e dois da Direção-Geral de Estatísticas de Educação e Ciência - DGEEC, sobre a Administração Pública Central e Regional e sobre as Câmaras Municipais), optou-se por distinguir entre comportamentos individuais e organizacionais, facto que proporciona um aumento da componente relativa ao contexto profissional neste Relatório.

Com este trabalho pretende-se não só analisar dados que careciam de um olhar mais profundo sobre a realidade portuguesa, como desenvolver uma compreensão abrangente e sintética sobre a vertente social da cibersegurança no país. Além das fontes mencionadas, o Eurobarómetro continua a ser uma referência muito importante neste documento. Todavia, muita da informação que diz respeito à educação e sensibilização é recolhida diretamente pelo Centro Nacional de Cibersegurança (CNCS). O equilíbrio entre as atitudes e os comportamentos, os níveis de cuidado em ciber-higiene, a comparação com a UE ou os esforços realizados para a educação e sensibilização são os aspetos mais relevados neste texto. O fator humano, como elemento transversal à cibersegurança, é especialmente convocado neste estudo.

O documento deste ano introduz uma análise global dos indicadores que pretende fornecer uma camada de interpretação acrescida. Considerando os dados e a experiência do CNCS, o texto procura oferecer uma base de informação para as decisões estratégicas quanto à educação e sensibilização dos indivíduos. Em termos de estrutura, o documento aplica um formato que privilegia a identificação do indicador, seguido de uma tabela com os números detalhados, um ou mais gráficos e um destaque com aspetos sublinhados. A terminar cada um dos três capítulos principais faz-se uma síntese. No final do documento, é possível consultar a Nota Metodológica com uma descrição das metodologias utilizadas pelas diversas fontes e pelo CNCS. Antes de se iniciar o capítulo sobre Atitudes, apresentam-se os Termos, Siglas e Abreviaturas, bem como a referida Análise Global.

D. TERMOS, SIGLAS E ABREVIATURAS

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

(adaptado de CNCS, *Relatório Sociedade 2019*)

Ciberbullying: "*bullying* realizado através da Internet ou telemóvel, envolvendo mensagens ofensivas ou maliciosas, *emails*, *chats* ou comentários, ou mesmo, em casos extremos, *websites* construídos com intenções maliciosas contra indivíduos ou certos grupos de pessoas".

(EC, *Internet Literacy Handbook*, 2017)

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

(ISO/IEC 27032)

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 2019-2023)

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

(ENISA *Overview of Cybersecurity and Related Terminology*, 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 2019-2023)

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

(adaptado de CNCS, *Relatório Sociedade 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, *Relatório Sociedade 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".

(NIST *Digital Identity Guidelines*. 2017)

Grandes Empresas: "empresas com 250 ou mais trabalhadores".

(Eurostat, 2020c)

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

(Lei nº 46/2018)

Médias Empresas: "empresas com 50 a 249 trabalhadores".

(Eurostat, 2020c)

Pequenas Empresas: "empresas com 10 a 49 trabalhadores".

(Eurostat, 2020c)

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, *Threat Landscape Report 2018*)

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, *Threat Landscape Report 2018*)

ANACOM: Autoridade Nacional de Comunicações.

AP Açores: Administração Pública Regional dos Açores.

AP Central: Administração Pública Central.

AP Madeira: Administração Pública Regional da Madeira.

CCIS: Consórcio Centro Internet Segura.

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.

IAPMEI: Agência para a Competitividade e Inovação.

INE: Instituto Nacional de Estatística.

IPDJ: Instituto Português do Desporto e Juventude.

IUTIC: Inquérito à Utilização das Tecnologias da Informação e da Comunicação.

IUTICAP: Inquérito à Utilização das Tecnologias da Informação e da Comunicação para a Administração Pública Central e Regional.

IUTICCM: Inquérito à Utilização das Tecnologias da Informação e da Comunicação para as Câmaras Municipais.

PP: pontos percentuais.

PT: Portugal.

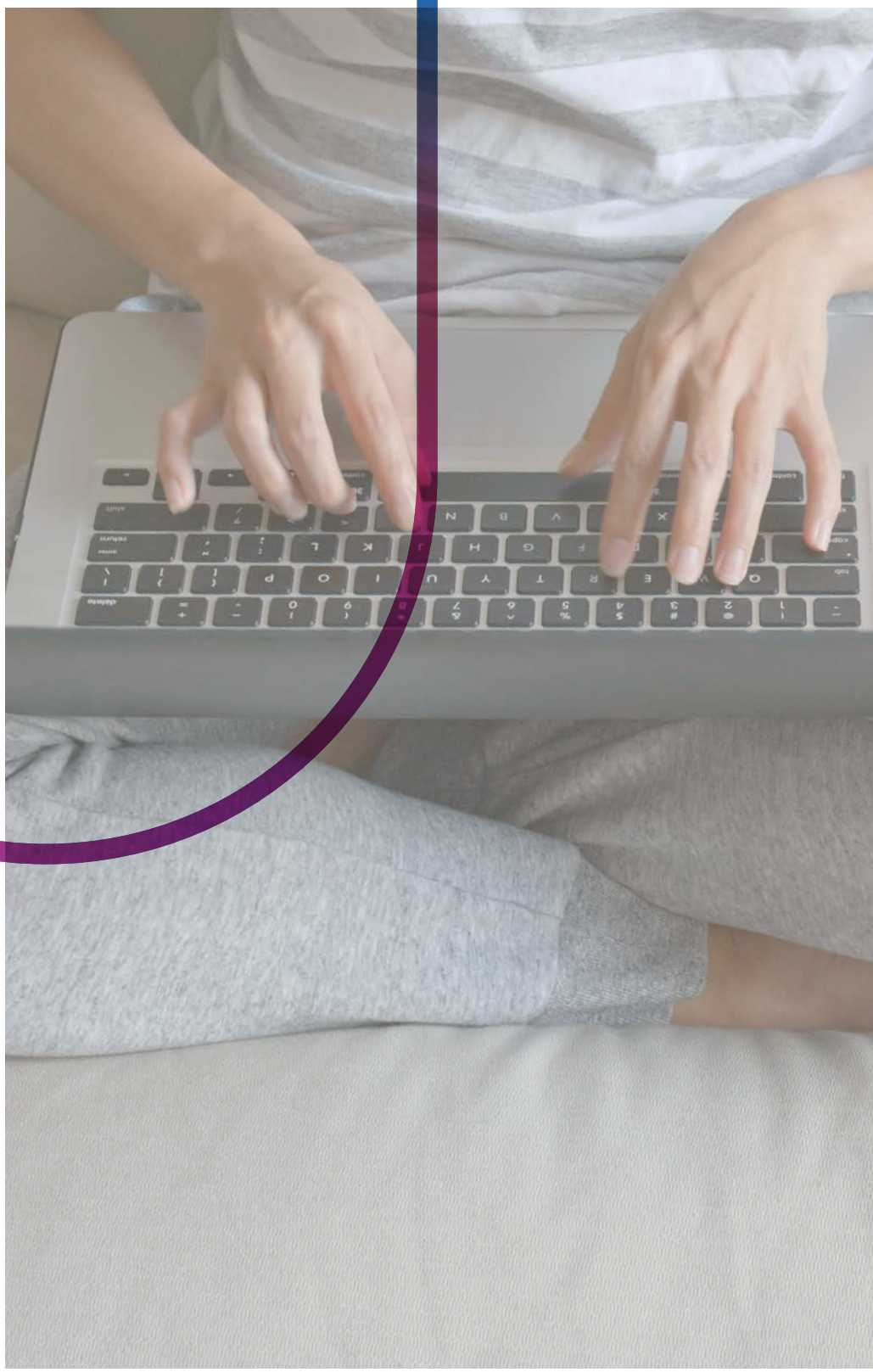
QNRCS: Quadro Nacional de Referência para a Cibersegurança.

RCMCS: Roteiro para Capacidades Mínimas de Cibersegurança.

TESP: Curso Técnico Superior Profissional.

TIC: Tecnologias de Informação e Comunicação.

UE: União Europeia (inclui Reino Unido).



E.

ANÁLISE GLOBAL

A análise global compreende uma síntese dos indicadores, com um quadro sintético que procura avaliar, à luz dos temas principais e de três critérios, o estado da cibersegurança em Portugal quanto ao tema "Sociedade". Inclui ainda uma articulação entre os resultados e as principais ameaças identificadas no *Relatório Cibersegurança em Portugal - Riscos & Conflitos 2020* (CNCS, 2020a). Por fim, estabelece uma integração destes dados no contexto da pandemia de Covid-19.

SÍNTESE DOS INDICADORES

Com base nos resultados e na seleção de alguns indicadores representativos, apresenta-se neste capítulo uma análise global dos quatro temas de referência (atitudes, comportamentos individuais, comportamentos organizacionais e educação e sensibilização) através da aplicação de três critérios de valoração: a) o absoluto, que verifica, em cada indicador, se os resultados positivos atingem pelo menos metade da amostra; b) o relativo, que compara os dados de cada indicador com a média da UE; e c) o da tendência, que assinala se a evolução do indicador é ou não positiva. O quadro e a análise que se seguem expõem uma síntese desta avaliação, mostrando os indicadores positivos somados em relação ao total analisado, tendo em conta os temas, os critérios e a soma global. Os resultados abaixo de 50% são considerados insuficientes. Para uma compreensão mais detalhada desta metodologia, ver caixa e anexo.

Quadro sintético de indicadores

Critérios/ Temas	a. Absoluto (+50%)	b. Relativo (+UE)	c. Tendência (+)	Resultado (-50%/+50%)
1. Atitudes	4 em 6 (67%)	1 em 6 (17%)	2 em 5 (40%)	7 em 17 (41%)
2. Comportamentos individuais	2 em 6 (33%)	1 em 6 (17%)	3 em 4 (75%)	6 em 16 (38%)
3. Comportamentos organizacionais	4 em 7 (57%)	1 em 3 (33%)	1 em 3 (33%)	6 em 13 (46%)
4. Educação e sensibilização	2 em 2 (100%)	0 em 1 (0%)	3 em 6 (50%)	5 em 9 (56%)
Resultado	12 em 21 (57%)	3 em 16 (19%)	9 em 18 (50%)	24 em 55 (44%)

Quadro 1

METODOLOGIA UTILIZADA NA CONSTRUÇÃO DO QUADRO SINTÉTICO DE INDICADORES

> Em relação a cada um dos 31 indicadores apresentados neste Relatório, seleciona-se o subindicador mais representativo (p. ex.: total com política de segurança) ou faz-se uma média de todos os subindicadores. Sobre este resultado, atribui-se um ou nenhum valor por cada um dos três critérios - desde que esse indicador represente, na sua evolução, algo benéfico, ou não indicie ambiguidades quanto ao que significa para melhorar a cibersegurança. De outro modo, não é considerado. No critério "absoluto", o valor é atribuído caso sejam igualados ou ultrapassados os 50% (exceto o indicador 21, que tem a relação inversa). No critério "relativo", o valor é atribuído sempre que seja ultrapassada ou igualada a média da UE. No critério "tendência", o valor é atribuído sempre que se verifique uma tendência avaliada como benigna (se a comparação com a UE for positiva, o valor da tendência é automaticamente positivo, mas apenas se esses dados cronológicos existirem).
>
> Para se chegar a um valor final, divide-se os valores atribuídos apenas pelo número de dados considerados. Um resultado é considerado positivo se ultrapassar os 50% dos pontos possíveis. Esta regra aplica-se aos resultados dos temas, mas também aos dos critérios, que podem ser lidos independentemente, além de permitir uma aplicação global. Para uma compreensão detalhada dos indicadores analisados, ver quadros em anexo.

Esta perspetiva permite mapear os conteúdos de educação e sensibilização a desenvolver, não só no ensino formal e não formal, como naquilo que decorre da formação e sensibilização em contexto de aplicação do QNRCS (em especial, Formação e Sensibilização e em várias medidas de Identificação) e do RCMCS (principalmente Fase II) (CNCS, 2019b e 2019c). De seguida, realiza-se uma análise detalhada dos temas e dos critérios, sublinhando destaques, apontando casos positivos e negativos, referenciando uma possível aplicação ao QNRCS e indicando os instrumentos do CNCS que podem ajudar a colmatar insuficiências.

ANÁLISE DOS TEMAS

1. ATITUDES

Destaque: importa melhorar a comparação de Portugal com a média da UE e a tendência anual em termos de atitudes em relação à cibersegurança.

Caso positivo: existe um aumento da preocupação com o cibercrime.

Caso negativo: verifica-se um nível baixo de informação percecionada sobre o risco de cibercrime.

Contributo para a aplicação do QNRCS: Proteger - PR.FC – Formação e Sensibilização.

Alguns instrumentos do CNCS: cursos *online* Cidadão Ciberseguro, Cidadão Ciberinformado e Consumidor Ciberseguro; Curso Geral de Cibersegurança; documentos de boas práticas.

> Fazendo uma análise global das atitudes, o resultado é insuficiente. Em 17 pontos possíveis, apenas se atingem 7 (41%). A componente em relação à qual os resultados são mais positivos é a dos números absolutos, onde, em 6, se atingem 4 (67%). A comparação com a UE é o critério em que os resultados são piores, com 1 em 6 (17%). Em termos de tendência, em 5 pontos possíveis, apenas se atingem 2 (40%).

2. COMPORTAMENTOS INDIVIDUAIS

Destaque: não obstante a tendência positiva, importa melhorar os comportamentos individuais em Portugal.

Caso positivo: os indivíduos alteram mais o seu comportamento em resultado de preocupações com a Internet do que anteriormente.

Caso negativo: os indivíduos ainda têm poucos cuidados com as *passwords*.

Contributo para a aplicação do QNRCS: Proteger - PR.FC Formação e Sensibilização.

Alguns instrumentos do CNCS: cursos *online* Cidadão Ciberseguro, Cidadão Ciberinformado e Consumidor Ciberseguro; Curso Geral de Cibersegurança; documentos de boas práticas.

> No que diz respeito ao comportamento individual, os resultados também são insuficientes, com 6 pontos em 16 possíveis (38%). O critério no qual o resultado é mais positivo, com 3 em 4 (75%), é o das tendências. Os dados absolutos apresentam valores menos positivos, com 2 em 6 (33%), e a comparação com a média da UE também, com 1 em 6 (17%).

3. COMPORTAMENTOS ORGANIZACIONAIS

Destaque: o comportamento organizacional, em Portugal, carece de melhoria.

Caso positivo: as empresas implementam muitas medidas de segurança das TIC em termos absolutos e comparando com a média da UE.

Caso negativo: as empresas definem insuficientemente políticas de segurança das TIC e a tendência é negativa.

Contributo para a aplicação do QNRCS: Identificar - ID.GV Governação; ID.AR Avaliação do risco; ID.GR Estratégia de gestão do risco.

Alguns instrumentos do CNCS: o RCMCS (permite ajudar as organizações a dar os primeiros passos no sentido de adquirirem as capacidades mínimas em cibersegurança).

> Os resultados dos comportamentos organizacionais estão aquém do desejável, com 6 pontos em 13 possíveis (46%). Ainda assim, os resultados absolutos são razoáveis, com 4 em 7 (57%). A comparação com a média da UE e a tendência anual registam ambas 1 ponto em 3 (33%). A este respeito, como se verifica, existem menos indicadores disponíveis do que em relação aos valores absolutos.

4. EDUCAÇÃO E SENSIBILIZAÇÃO

Destaque: a educação e sensibilização, em Portugal, apresenta uma tendência positiva.

Caso positivo: o número de cursos em Cibersegurança e Segurança de Informação e de alunos que se inscreveram nestes cursos está a aumentar.

Caso negativo: a percentagem de mulheres que se inscreveram e que se diplomaram nestes cursos relativamente ao total dos que se inscreveram e diplomaram está a diminuir.

Contributo para a aplicação do QNRCS: Proteger - PR.FC – Formação e Sensibilização.

Alguns instrumentos do CNCS (como ofertas para a sensibilização): cursos *online* Cidadão Ciberseguro, Cidadão Ciberinformado e Consumidor Ciberseguro; Curso Geral de Cibersegurança.

> Os resultados mais positivos em relação aos quatro temas sob análise são os da educação e sensibilização, com 5 pontos em 9 possíveis (56%). Não obstante, estes dados estão limitados quanto à definição de um critério para os valores absolutos e à comparação com a UE: o primeiro, com dois dados disponíveis e, o segundo, com apenas um. Os 100% do critério absoluto e os 0% do relativo devem ser lidos à luz destas limitações. Quanto a tendências, elas atingem 3 pontos em 6 (50%), o que, dada a quantidade de dados disponíveis, se reveste de alguma relevância.

ANÁLISE DOS CRITÉRIOS

A. ABSOLUTO

Destaque: resultados absolutos suficientes, em Portugal, mas com margem para crescerem.

Caso positivo: em termos absolutos, as atitudes e os comportamentos organizacionais são positivos.

Caso negativo: os comportamentos individuais apresentam valores absolutos baixos.

> Quanto aos resultados absolutos, atingem-se 12 pontos em 20 possíveis (57%). Os temas com melhores resultados são as atitudes, com 4 em 6 (67%), e a educação e sensibilização, com 2 em 2 (100%), embora este último apenas com dois dados disponíveis. Ao nível dos comportamentos individuais, os resultados são insuficientes, com 2 em 6 (33%). Os comportamentos organizacionais, por sua vez, atingem valores positivos, com 4 em 7 (57%).

B. RELATIVO

Destaque: em comparação, Portugal fica frequentemente abaixo do nível médio da UE.

Caso positivo: o comportamento organizacional compara um pouco melhor com a média da UE do que os outros temas, mas de forma insuficiente.

Caso negativo: as atitudes e os comportamentos individuais apresentam índices quase sempre inferiores à média da UE.

> Em termos relativos os resultados são notoriamente insuficientes, com 3 em 16 (19%). A comparação com a UE revela-se particularmente aquém do desejável ao nível das atitudes e dos comportamentos individuais, ambos com 1 em 6 (17%). Em termos de comportamentos organizacionais, a comparação é ligeiramente melhor, com 1 em 3 (33%), mas limitada pelo número de dados disponíveis. O único valor em educação e sensibilização comparável com a média da UE é insuficiente.

C. TENDÊNCIA

Destaque: em Portugal, as tendências são minimamente positivas.

Caso positivo: destacam-se os comportamentos individuais, que têm melhorado em termos de tendência, embora comparem mal com a média da UE.

Caso negativo: os comportamentos organizacionais têm uma tendência menos positiva.

> As tendências apresentam resultado positivo, com 9 pontos em 18 possíveis (50%). Os melhores resultados são visíveis ao nível dos comportamentos individuais, com 3 em 4 (75%) e na educação e sensibilização, com 3 em 6 (50%). Os resultados menos positivos são os das atitudes, com 2 em 5 (40%), bem como os dos comportamentos organizacionais, com 1 em 3 (33%).

Tendo em conta o exposto, verifica-se que o único tema positivo é a educação e sensibilização. Nos critérios os valores absolutos e as tendências também são positivos. Isto significa que existe um esforço para melhorar a ciber-higiene dos indivíduos e das organizações e que há um potencial para que o país venha a ter mais maturidade neste domínio. Todavia, ainda há trabalho a realizar no que diz respeito às consequências em matéria de atitudes e comportamentos efetivos, sobretudo comparando com a média da UE. O resultado global da componente "Sociedade" é insuficiente, com 24 pontos em 55 possíveis (44%).

CIBERAMEAÇAS RELACIONADAS COM O COMPORTAMENTO INDIVIDUAL

No *Relatório Cibersegurança em Portugal - Riscos & Conflitos 2020* (CNCS, 2020a) destacaram-se como ciberameaças particularmente relevantes para o ciberespaço de interesse nacional (as de primeiro nível) o *phishing* e o *software* malicioso. Tendo em conta esse diagnóstico, que se reproduz noutras fontes a nível internacional (ENISA, 2020), é possível selecionar alguns indicadores sobre comportamento individual que se relacionam muito diretamente com estas ciberameaças, embora, na realidade, todos os indicadores contribuam para compreender a resiliência humana neste domínio.

Observando alguns indicadores específicos do Eurobarómetro 499, verificam-se referências relevantes ao *phishing* e ao *software* malicioso. Atenda-se, nomeadamente, aos seguintes indicadores: 4, relativo às preocupações com certos cibercrimes; 7, em relação ao que fariam os indivíduos no caso de serem vítimas de algumas ciberameaças; 8, sobre as alterações de comportamento fruto da preocupação com a Internet; e 11, referente ao que os indivíduos realmente fizeram quando foram vítimas de certas ciberameaças.

Quadro de indicadores diretamente relacionados com as ciberameaças de primeiro nível

	Indicador 4 Preocupação com...	**Indicador 7** Fariam alguma coisa caso fossem vítimas de...	**Indicador 8** Não abrem *emails* desconhecidos... e instalaram antivírus...	**Indicador 11** Fizeram alguma coisa quando foram vítimas de...
Phishing	65% em PT (+2 pp do que 2018); 59% na média da UE.	72% em PT (+16 do que 2018); 67% na média da EU.	43% em PT (-1 pp do que 2018); 42% na média da UE.	61% em PT (+9 pp do que 2018); 43% na média da UE.
Software malicioso	76% em PT (+1 pp do que 2018); 66% na média da UE.	71% em PT (-1 pp do que 2018); 70% na média da UE.	35% em PT (-9 pp do que 2018); 42% na média da UE.	65% em PT (-18 pp do que 2018); 52% na média da UE.

Quadro 2

Considerando o quadro 2, verifica-se que, em relação ao *phishing*, em geral, os indicadores, exceto o 8, apresentam valores acima dos 50%, bem como da média da UE, e a tendência é de melhoria. O indicador mais negativo é, portanto, o 8, que diz respeito aos cuidados a ter antes de o incidente ocorrer, nomeadamente não abrir *emails* de pessoas desconhecidas.

No que diz respeito ao *software* malicioso, o indicador 8, referente à instalação de *software* antivírus, continua a ser o mais negativo, com um valor abaixo dos 50%, com tendência negativa e com resultado inferior à média da UE. Quanto aos outros indicadores, os resultados são em geral positivos, excetuando algumas tendências decrescentes. De referir que existem mais ações que podem prevenir o *software* malicioso, como, entre outras, não abrir *emails* de origem desconhecida, visto muitas vezes o *phishing* trazer *software* malicioso.

Os dados do indicador 8 sobre as duas ciberameaças, um indicador da prática e da prevenção, mostram a importância de, nas ações de educação e sensibilização, se insistir nas boas práticas em termos de prudência, independentemente da consciência e capacidade de reação de que os indivíduos possam dispor (acresce que o quadro sintético mostra que as atitudes também são insuficientes em termos globais).

O CASO COVID-19

Ainda que este Relatório incida sobretudo no ano de 2019, não se deve ignorar o efeito que a pandemia de Covid-19 pode ter nos indicadores apresentados. Ainda que os números possam sofrer alterações importantes fruto desta realidade, indicam, todavia, o nível de preparação dos indivíduos relativamente às principais ciberameaças colocadas pela pandemia.

Dados da ANACOM mostram que o consumo do serviço de Internet fixa aumentou 61,1% no primeiro semestre de 2020, comparando com o mesmo semestre do ano anterior (ANACOM, 2020). Um aumento que poderá estar relacionado com as mudanças na organização do trabalho, do ensino e dos transportes provocadas pelas medidas de combate à pandemia, as quais promoveram o trabalho e a aprendizagem à distância, o isolamento dos indivíduos, uma maior dependência dos serviços digitais e um uso mais frequente de computadores portáteis e dispositivos móveis, fornecidos ou não pela entidade empregadora ou escolar. Esta circunstância favoreceu o aumento de ciberataques oportunistas.

Internacionalmente, foi identificado o crescimento de algumas ciberameaças relacionadas com a pandemia, tais como campanhas de *phishing*; infeção por *software* malicioso, algum dele *ransomware*; aplicações fraudulentas; desinformação; ou fraudes digitais para a compra de materiais médicos (CNCS, 2020a e 2020b). Em Portugal, tendo em conta os dados publicados pelo Observatório de Cibersegurança ao longo de 2020, verifica-se um crescimento significativo do número de incidentes registados pelo CERT.PT, em cerca 101%, se compararmos o primeiro semestre de 2020 com o período homólogo do ano anterior (CNCS, 2020c). Um dos aspetos mais relevantes destes dados é o contributo do *phishing* para este aumento. Este tipo de incidente foi o mais frequente até agosto de 2020, correspondendo a 36% dos incidentes registados (em 2019, o valor foi de 31% no final do ano, sendo que o *phishing* também foi o tipo de incidente que mais se notabilizou) (CNCS, 2020a e 2020d).

Numa análise realizada ao *phishing* registado pelo CERT.PT durante o segundo trimestre de 2020, concluiu-se que apenas 1% das campanhas lançadas utilizaram a Covid-19 como "tema-gancho" e que cerca de 37% afetaram o setor bancário. A técnica de persuasão mais usada, como é típico do *phishing* bancário, foi a presumível autoridade e credibilidade

do emissor (CNCS, 2020c). A referência ao *phishing* e a este *modus operandi* é relevante porque mostra a importância da engenharia social como instrumento de ataque por parte dos agentes de ameaças. Enquanto técnica de manipulação, a engenharia social confronta a preparação das atitudes e a consistência dos comportamentos. Considerando os dados globais apresentados, é evidente que existem vários aspetos a melhorar nas atitudes e no comportam das pessoas no âmbito do ciberespaço. Em relação ao *phishing* e ao *software* malicioso (o segundo tipo de incidente mais frequente no ano passado e durante o primeiro semestre de 2020, atrás do *phishing*), sublinhe-se, de novo, a importância de se explicar o que se deve fazer para prevenir incidentes, promovendo a passagem da atitude ao comportamento, para lá da preocupação ou da reação. Esta ideia deve ressoar na construção das estratégias para a resiliência do ciberespaço, num tempo em que este ganha uma importância acrescida.

Por fim, é importante referir a possível articulação entre certos indicadores e as compras *online*. Alguns números mostram que a propensão para o hábito de comprar *online*, que a pandemia pode implicar, encontra algumas barreiras de segurança em termos de atitudes e comportamentos. Por exemplo, em Portugal, em 2019, verifica-se, entre os indivíduos, alguma preocupação com a partilha de dados pessoais neste contexto (54%), mais do que a média da UE (46%) (Eurobarómetro 499). Além disso, os indivíduos, em Portugal, evitam mais comprar *online* devido a preocupações com a segurança de pagamento (23%) do que a média da UE (6%) (Eurostat, 2020a). O efeito real destas premissas ligadas à segurança nas compras *online* só poderá ser convenientemente avaliado com dados mais completos sobre o ano 2020.

De referir que os cursos *online* do CNCS Cidadão Ciberseguro, Cidadão Ciberinformado e Consumidor Ciberseguro são instrumentos úteis e acessíveis para reforçar as atitudes e os comportamentos dos indivíduos em termos da sua resiliência em relação às principais ciberameaças, em particular no contexto da pandemia de Covid-19.

CNCS
Centro Nacional de Cibersegurança PORTUGAL

ATITUDES

Observatório de **Cibersegurança**

As atitudes são fundamentais para compreender as predisposições das pessoas para adotarem os comportamentos mais seguros. Dado o seu caráter psicossocial, neste capítulo, recolhem-se indicadores sobre os indivíduos e não sobre as organizações, embora as atitudes dos indivíduos ajudem a moldar o comportamento organizacional. A fonte utilizada é o Eurobarómetro Especial 499 *Europeans' attitudes towards cyber security*, publicado em 2020, com dados referentes a 2019. Recorre-se também a todos os Eurobarómetros anteriores com a mesma temática. As atitudes analisadas dizem respeito às preocupações com a cibersegurança, ao nível de informação que se perceciona possuir, ao conhecimento sobre outras vítimas de cibercrime ou à predisposição para reagir a ciberameaças.

1. Que preocupações têm os indivíduos, em Portugal, se alguma, em relação ao uso da Internet para atividades como o banco *online* ou a compra de bens e serviços *online*? (Múltiplas respostas possíveis) *Utilizadores de Internet*. (%)

	PT 2019	UE (tendência 2018-2019)	Tendência PT (2018-2019)	Tendência PT (2017-2018)	Tendência PT (2014-2017)	Tendência PT (2013-2014)
A segurança dos pagamentos online	32	41 (-2)	-6	-9	+11	+1
O uso indevido dos dados pessoais	54	46 (+3)	+5	-2	+21	+1
Não poder inspecionar os bens ou pedir conselho a uma pessoa real	14	22 (-2)	-1	-13*	-18	-3
Tem medo de não receber os produtos ou serviços comprados online	20	22 (-1)	-15	=	+18	+3
Outra	6	10 (+5)	+4	**	**	+1
Nenhuma preocupação	21	15 (-4)	+1	**	**	+5
Não sabe	5	6 (+4)	+3	**	**	+1

* A formulação da pergunta alterou ligeiramente de 2017 para 2018, por isso esta diferença é relativa.
** Dados indisponíveis.

Tabela 1 | Eurobarómetro 499, 480, 464a, 423 e 404

Aspetos sociodemográficos relevantes em Portugal, 2019[2]

Sexo 80% dos homens portugueses têm pelo menos uma preocupação, enquanto nas mulheres este valor é de 67%.

Idade Os indivíduos com idades compreendidas entre os 25 e os 39 anos manifestam ter mais preocupações do que os indivíduos das restantes faixas etárias, com 78% a revelarem ter pelo menos uma preocupação.

Educação Os indivíduos que terminaram os estudos com mais de 20 anos e aqueles que ainda estudam são os que apresentam percentagens maiores quanto a ter pelo menos uma preocupação, com 86% e 78%, respetivamente.

UE Diferentemente de Portugal, na média da UE, a percentagem de mulheres com pelo menos uma preocupação é ligeiramente superior à dos homens, com 82% e 77%, respetivamente. As faixas etárias e os diferentes níveis de educação também são mais homogéneos entre si.

Eurobarómetro 499

2 Nos Eurobarómetros, os grupos etários correspondem aos seguintes intervalos: 15-24 anos; 25-39 anos; 40-54 anos; +55 anos. Os grupos educacionais, aos seguintes tipos: estudaram até aos 15 anos; até aos 16-19 anos; até depois dos 20 anos; ainda estudam. Quando se refere "Todos os indivíduos" entende-se todas as faixas etárias, quer usem quer não usem a Internet.

Que preocupações têm os indivíduos, em Portugal, se alguma, em relação ao uso da Internet para atividades como o banco *online* ou a compra de bens e serviços *online*? (Múltiplas respostas possíveis) 2013-2019. *Utilizadores de Internet*. (%)

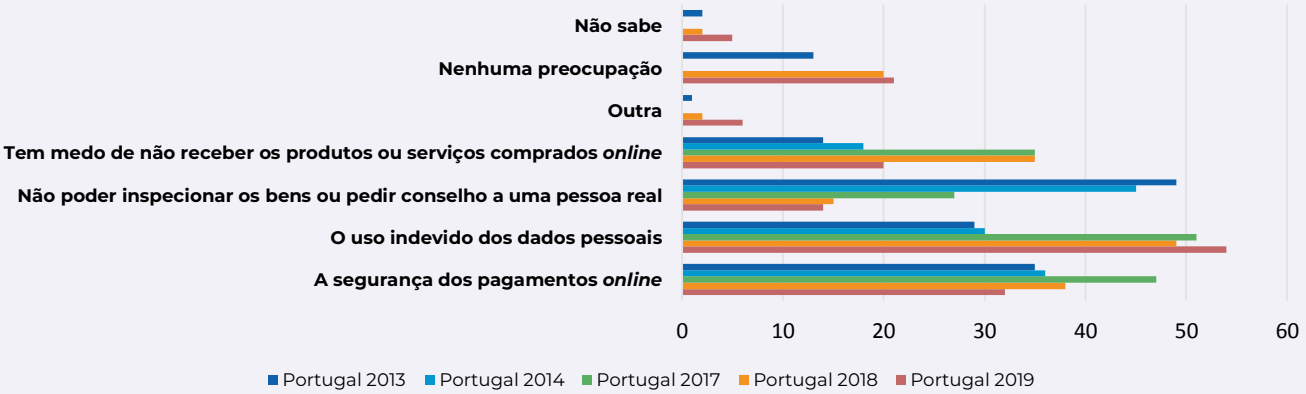


Figura 1 | Eurobarómetro 499, 480, 464a, 423 e 404

Que preocupações têm os indivíduos, em Portugal, se alguma, em relação ao uso da Internet para atividades como o banco *online* ou a compra de bens e serviços *online*? (Múltiplas respostas possíveis) Comparação com UE. *Utilizadores de Internet*. (%)

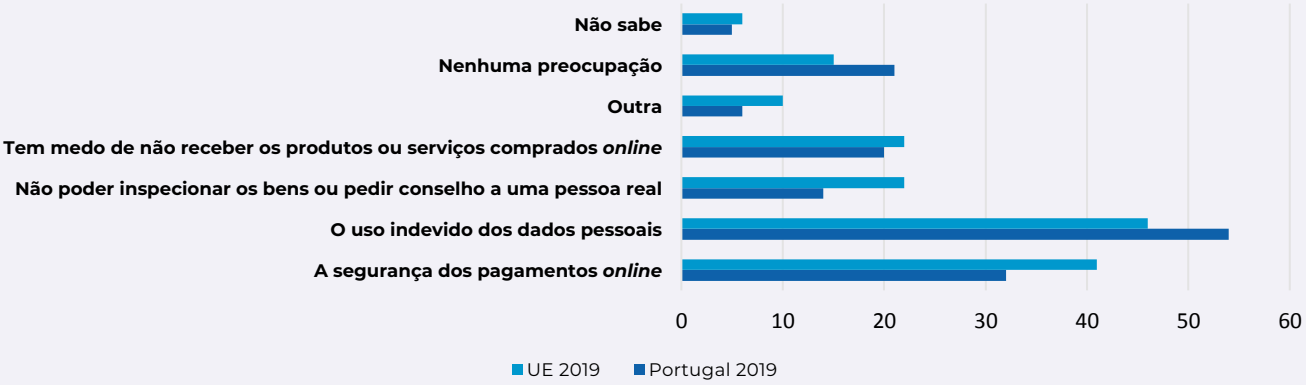


Figura 2 | Eurobarómetro 499

Que preocupações têm os europeus, se alguma, em relação ao uso da Internet para atividades como o banco *online* ou a compra de bens e serviços *online*? (Múltiplas respostas possíveis) 2018-2019. *Utilizadores de Internet*. (%)

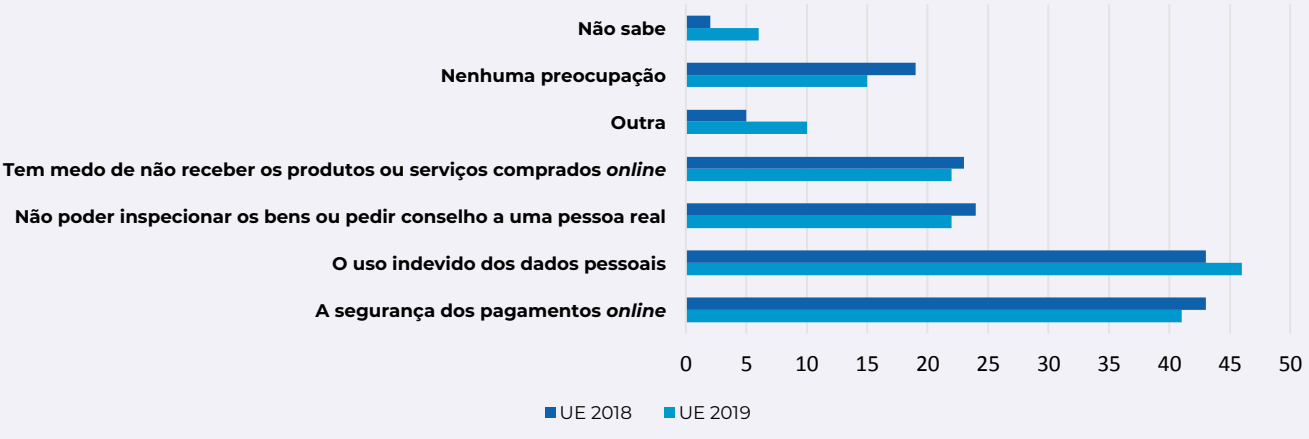


Figura 3 | Eurobarómetro 499 e 480

Destaques

Em relação ao uso da Internet para atividades como o banco *online* ou a compra de bens e serviços *online*, de entre as preocupações apresentadas, para os indivíduos, em Portugal, o uso indevido dos dados pessoais (54%) é a maior delas, mais do que a média da UE (46%) – o valor em Portugal aumentou 5 pp em relação ao ano anterior;

Não obstante, a média da UE é superior aos valores registados em Portugal quanto às outras preocupações, sendo que 74% dos respondentes têm alguma preocupação, enquanto a média da UE é de 79% (subtraídos os que revelam "nenhuma preocupação" ou "não sabem");

A discrepância mais acentuada entre 2018 e 2019 é a que diz respeito à diminuição em 15 pp dos que têm medo de não receber produtos ou serviços comprados *online*;

Em Portugal, existem mais variações sociodemográficas do que na média da UE, com destaque, quanto a um maior número de preocupações, para os homens, a faixa etária entre os 25 e os 39 anos e os indivíduos com mais estudos.

2. Quão bem informados se sentem os indivíduos, em Portugal, quanto ao risco de cibercrime? ***Todos os indivíduos.*** **(%)**

	PT 2019	UE (tendência 2018-2019)	Tendência PT (2018-2019)	Tendência PT (2017-2018)	Tendência PT (2014-2017)	Tendência PT (2013-2014)
Muito bem informado	2	11 (+1)	-1	-3	+1	+1
Razoavelmente bem informado	39	41 (=)	-4	+1	+3	+12
Não muito bem informado	34	30 (+2)	+4	+1	+6	-10
Nada informado	23	17 (-1)	+1	=	-10	-3
Não sei	2	1 (-2)	=	+1	=	=

Tabela 2 | Eurobarómetro 499, 480, 464a, 423 e 404

Aspetos sociodemográficos relevantes em Portugal, 2019

Sexo Os homens sentem-se mais bem informados do que as mulheres. Por exemplo, 47% sentem-se razoavelmente bem informados, enquanto apenas 33% das mulheres se sentem desse modo.

Idade Os indivíduos com mais de 55 anos sentem-se menos informados do que os indivíduos das restantes faixas etárias. Por exemplo, 51% destes indivíduos sentem-se nada informados, mais do que qualquer das restantes faixas etárias.

Educação Os indivíduos que estudaram no máximo até aos 15 anos de idade sentem-se pior informados do que os restantes. Por exemplo, 50% destes indivíduos sentem-se nada informados, mais do que qualquer dos outros grupos, que estudaram mais anos ou ainda estudam.

UE Tendências alinhadas com a média da UE.

Eurobarómetro 499

Quão bem informados se sentem os indivíduos, em Portugal, quanto ao risco de cibercrime? 2013-2019. *Todos os indivíduos.* (%)

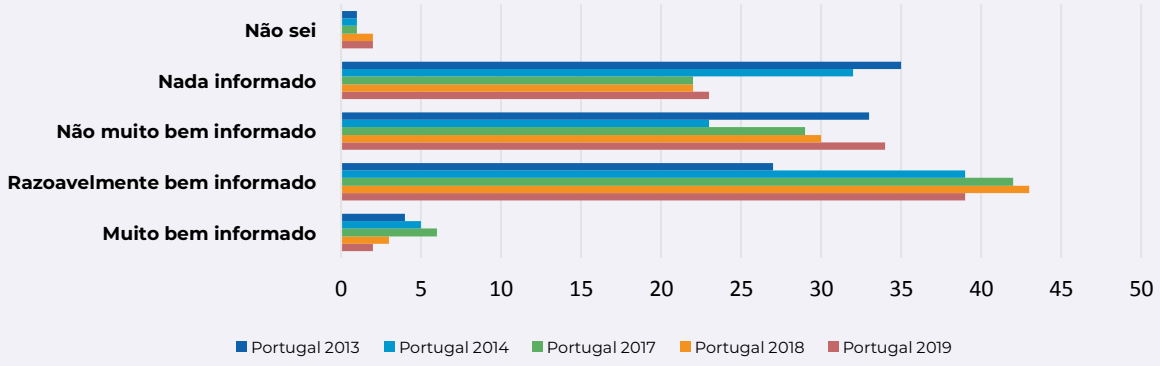


Figura 4 | Eurobarómetro 499, 480, 464a, 423 e 404

Quão bem informados se sentem os indivíduos, em Portugal, quanto ao risco de cibercrime? Comparação com a UE. *Todos os indivíduos*. (%)

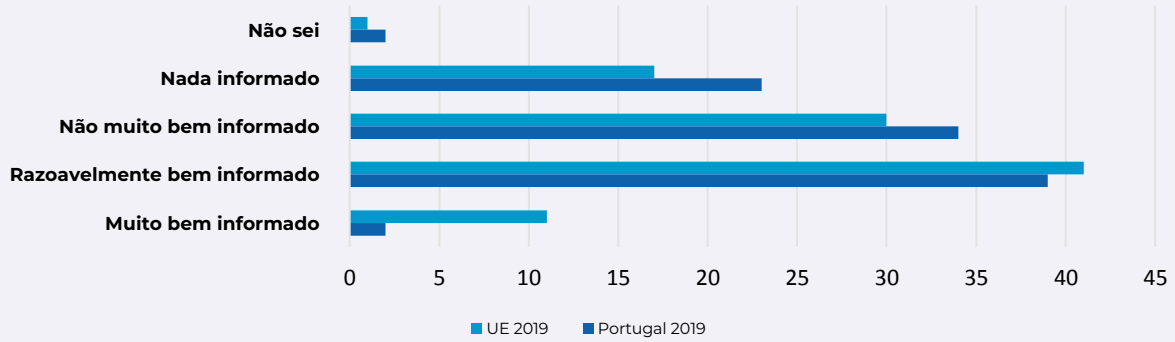


Figura 5 | Eurobarómetro 499

Quão bem informados se sentem os europeus quanto ao risco de cibercrime? 2018-2019. *Todos os indivíduos*. (%)

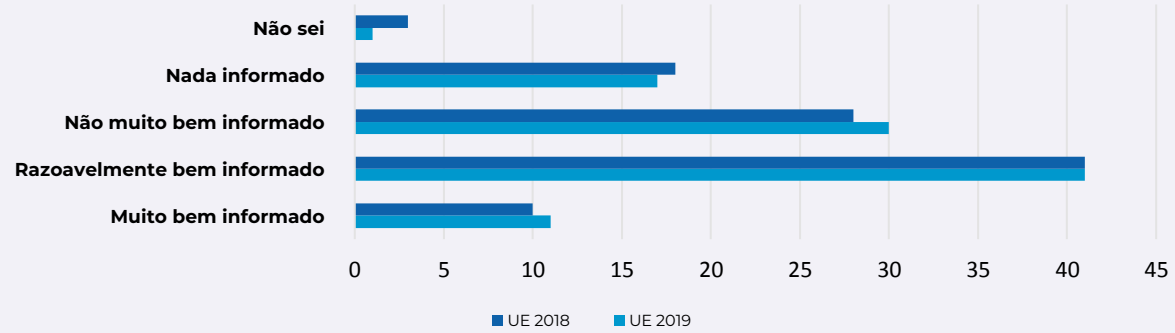


Figura 6 | Eurobarómetro 499 e 480

DESTAQUES

Entre 2018 e 2019, há um decréscimo na percentagem de indivíduos, em Portugal, que se sentem muito bem informados (2%, isto é, menos 1 pp) ou razoavelmente bem informados (39%, ou seja, menos 4 pp);

39% dos indivíduos, em Portugal, sentem-se razoavelmente bem informados, 34% não muito bem informados e 23% nada informados;

A média da UE é superior no que diz respeito a estar bem informado, particularmente entre os que se consideram muito bem informados: 11% na UE e 2% em Portugal;

O perfil do indivíduo que se sente bem informado em Portugal tende a corresponder a um homem, jovem e com mais estudos.

3. Em que medida os indivíduos, em Portugal, concordam com cada uma das seguintes afirmações? Concordam. *Todos os indivíduos*. (%)

	PT 2019	UE (tendência 2018-2019)	Tendência PT (2018-2019)	Tendência PT* (2014-2017)	Tendência PT* (2013-2014)
É capaz de se proteger o suficiente contra o cibercrime	73	78 (-1)	=	+3	+2
Está preocupado de que a sua informação pessoal não seja mantida segura pelas autoridades públicas	66	76 (-3)	=	+1	+12**
Está preocupado de que a sua informação pessoal não seja mantida segura pelos websites	66	68 (=)	+2	+2	+9
Acredita que o risco de ser vítima de cibercrime está a aumentar	64	61 (-1)	+2	+3	+10
Evita revelar informação pessoal online	45	52 (-9)	-8	-8	***

* Só a partir do inquérito referente a 2018 é que as perguntas começaram a ser realizadas a todos os inquiridos e não apenas aos utilizadores de Internet. Optou-se por fazer comparações diretas apenas entre os inquéritos com bases iguais, daí compararem-se os dados entre 2013 e 2017 e entre 2018 e 2019 separadamente.
** No inquérito de 2013 esta pergunta refere-se ao último ano.
*** Pergunta não realizada no inquérito de 2013.

Tabela 3 | Eurobarómetro 499, 480, 464a, 423 e 404

Aspetos sociodemográficos relevantes em Portugal, 2019

Sexo Sem diferenças relevantes entre sexos.

Idade Os indivíduos com mais de 55 anos de idade tendem a concordar menos com as afirmações apresentadas. Por exemplo, apenas 25% destes indivíduos concordam que conseguem proteger-se o suficiente contra o cibercrime, abaixo dos restantes grupos etários.

Educação Os indivíduos que estudaram no máximo até aos 15 anos de idade tendem a concordar menos com as afirmações apresentadas. Por exemplo, apenas 22% destes indivíduos concordam que conseguem proteger-se o suficiente contra o cibercrime, abaixo dos restantes grupos educacionais.

UE Tendências alinhadas com a média da UE.

Eurobarómetro 499

Em que medida os indivíduos, em Portugal, concordam com cada uma das seguintes afirmações? Concordam. 2018-2019. *Todos os indivíduos*. (%)

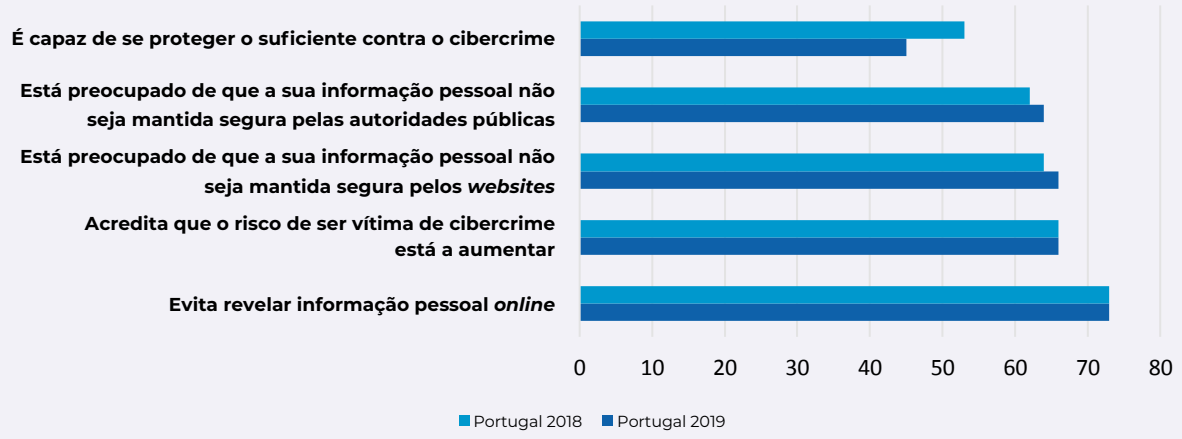


Figura 7 | Eurobarómetro 499 e 480

Em que medida os indivíduos, em Portugal, concordam com cada uma das seguintes afirmações? Concordam. Comparação com UE. *Todos os indivíduos*. (%)

Figura 8 | Eurobarómetro 499

Em que medida os europeus concordam com cada uma das seguintes afirmações? Concordam. 2018-2019. *Todos os indivíduos*. (%)

Figura 9 | Eurobarómetro 499 e 480

DESTAQUES

73% dos indivíduos, em Portugal, afirmam evitar revelar informação pessoal *online*, a afirmação com a qual mais concordaram, em alinhamento com o ano anterior;

A maior discrepância de valores em relação à média da UE diz respeito aos que acreditam que o risco de ser vítima de cibercrime está a aumentar: em Portugal, 66% dos inquiridos concordam com esta afirmação; na UE, o valor atinge os 76%;

Quer em Portugal, quer na média da UE, há um decréscimo assinalável, em relação ao ano anterior, entre os que afirmam ser capazes de se proteger o suficiente contra o cibercrime – menos 8 pp em Portugal (45%) e menos 9 pp na média da UE (52%);

Os indivíduos, em Portugal, com mais de 55 anos e os que estudaram no máximo até aos 15 anos de idade tendem a concordar menos com as afirmações apresentadas.

4. Os cibercrimes incluem muitos tipos de atividade criminal. Quão preocupados estão os indivíduos, em Portugal, pessoalmente, acerca de experienciar ou ser vítima das seguintes situações? Preocupados. *Utilizadores de internet.* (%)

	PT 2019	UE (tendência 2018-2019)	Tendência PT (2018-2019)	Tendência PT (2017-2018)	Tendência PT (2014*-2017)	Tendência PT (2013-2014)
A infeção de dispositivos com software malicioso (vírus, etc.)	76	66 (-5)	+1	+4	-1	**
Roubo de identidade (alguém roubar os dados pessoais e fazer-se passar por si)	77	66 (-4)	+9	-1	-5	+15
Fraude em cartão bancário ou em banco online	74	67 (-3)	+10	+2	=	+20
Acidentalmente, encontrar material com abuso sexual infantil online	65 ***	53 (-14)	+4	=	-6	+20
Hacking a redes sociais online ou conta de email	73	61 (-6)	+6	+1	-6	+19
Material online que promove ódio racial ou extremismo religioso	59	53 (-12)	+1	+3	-4	+12
Ciberataques que impedem o seu acesso a serviços online, como banca ou serviços públicos	60	57 (-4)	=	+5	-1	+9
Exigência de um pagamento em troca da recuperação do controlo sobre o seu dispositivo	65	55 (-5)	+5	+2	-1	**
Emails fraudulentos ou telefonemas a pedir os seus dados pessoais	65	59 (-1)	+2	+3	-6	+13
Fraude online em que os bens adquiridos não são entregues, são contrafeitos ou não são como publicitados	67	54 (-4)	+6	+2	-3	+16

* O fraseado de algumas perguntas está ligeiramente diferente no inquérito de 2014.
** Pergunta não realizada em 2013.
*** Pergunta ligeiramente alterada em 2019 em relação ao ano anterior.

Tabela 4 | Eurobarómetro 499, 480, 464a, 423 e 404

Aspetos sociodemográficos relevantes em Portugal, 2019

Sexo As mulheres apresentam em todos os casos percentagens ligeiramente superiores aos homens no que diz respeito às preocupações em causa. Por exemplo, 67% das mulheres e 63% dos homens estão preocupados com *emails* fraudulentos ou telefonemas a pedir os dados pessoais.

Idade Verifica-se uma tendência para que os indivíduos com mais de 55 anos de idade manifestem menos preocupações do que os restantes. Por exemplo, 50% destes indivíduos mostram-se preocupados com a possibilidade de ocorrerem ciberataques que impeçam o seu acesso a serviços *online*, como banca ou serviços públicos, abaixo dos restantes grupos etários.

Educação Os indivíduos que estudaram no máximo até aos 15 anos de idade tendem a manifestar menos preocupações. Por exemplo, 47% destes indivíduos mostram-se preocupados com a possibilidade de ocorrerem ciberataques que impeçam o seu acesso a serviços *online*, como banca ou serviços públicos, abaixo dos restantes grupos etários.

UE Os indivíduos com idades compreendidas entre os 15 e os 24 anos tendem a ter menos preocupações na média da UE do que em Portugal. Por exemplo, apenas 51% na média da UE estão preocupados com *emails* fraudulentos ou telefonemas a pedir os seus dados pessoais, enquanto em Portugal esse valor atinge os 72% nesta faixa etária. No que diz respeito à educação, na média da UE, não se observa a mesma discrepância entre grupos que se verifica em Portugal, a qual mostra menor preocupação por parte dos indivíduos que estudaram até aos 15 anos de idade. Por exemplo, entre estes, 61%, na média da UE, estão preocupados com *emails* fraudulentos ou telefonemas a pedir os dados pessoais, o valor mais elevado, enquanto em Portugal esse valor atinge apenas os 55% e é o mais baixo comparando com os restantes grupos.

Os cibercrimes incluem muitos tipos de atividade criminal. Quão preocupados estão os indivíduos, em Portugal, pessoalmente, acerca de experienciar ou ser vítima das seguintes situações? Preocupados. 2013-2019. *Utilizadores de Internet*. (%)

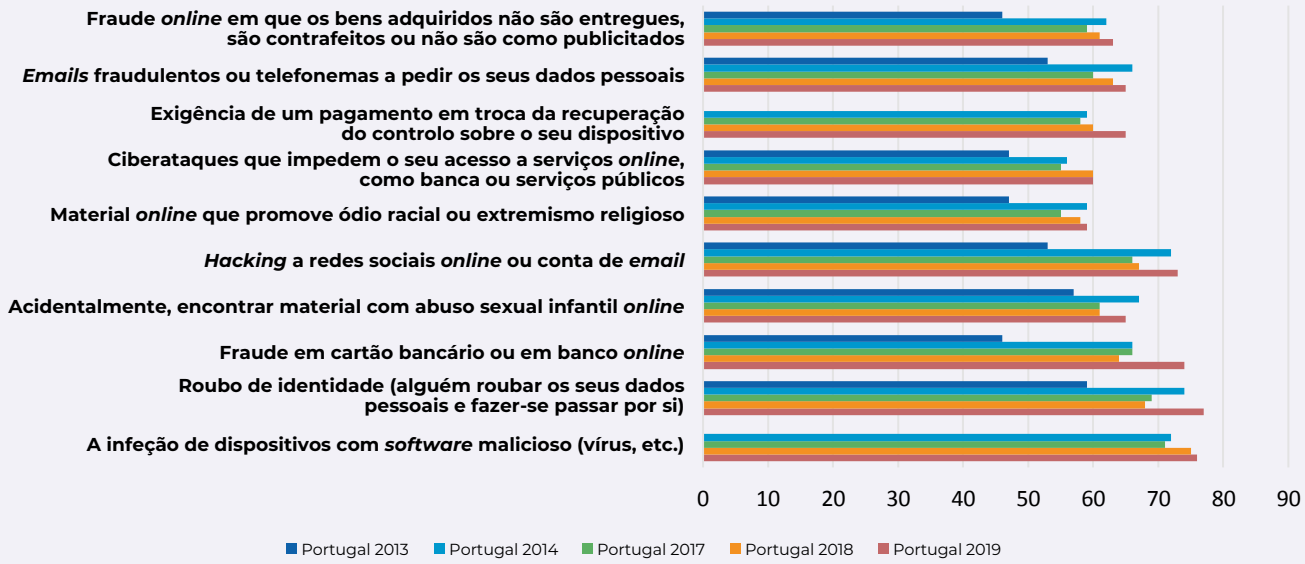


Figura 10 | Eurobarómetro 499, 480, 464a, 423 e 404

Os cibercrimes incluem muitos tipos de atividade criminal. Quão preocupados estão os indivíduos, em Portugal, pessoalmente, acerca de experienciar ou ser vítima das seguintes situações? Preocupados. Comparação com UE. *Utilizadores de Internet*. (%)

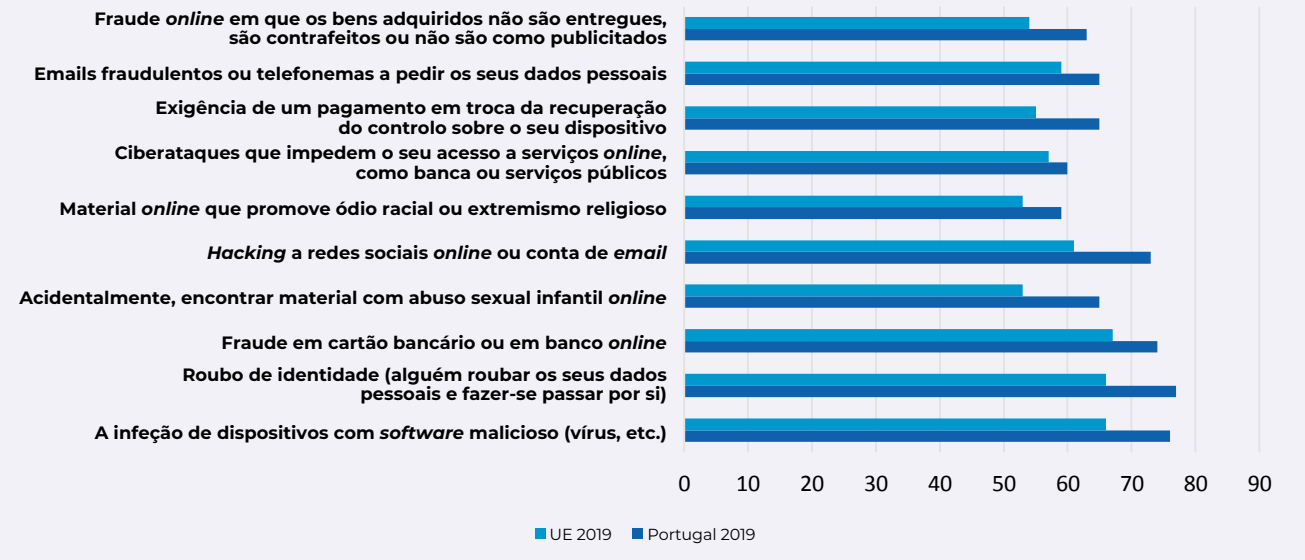


Figura 11 | Eurobarómetro 499

Os cibercrimes incluem muitos tipos de atividade criminal. Quão preocupados estão os europeus, pessoalmente, acerca de experienciar ou ser vítima das seguintes situações? Preocupados. 2018-2019. *Utilizadores de Internet.* (%)

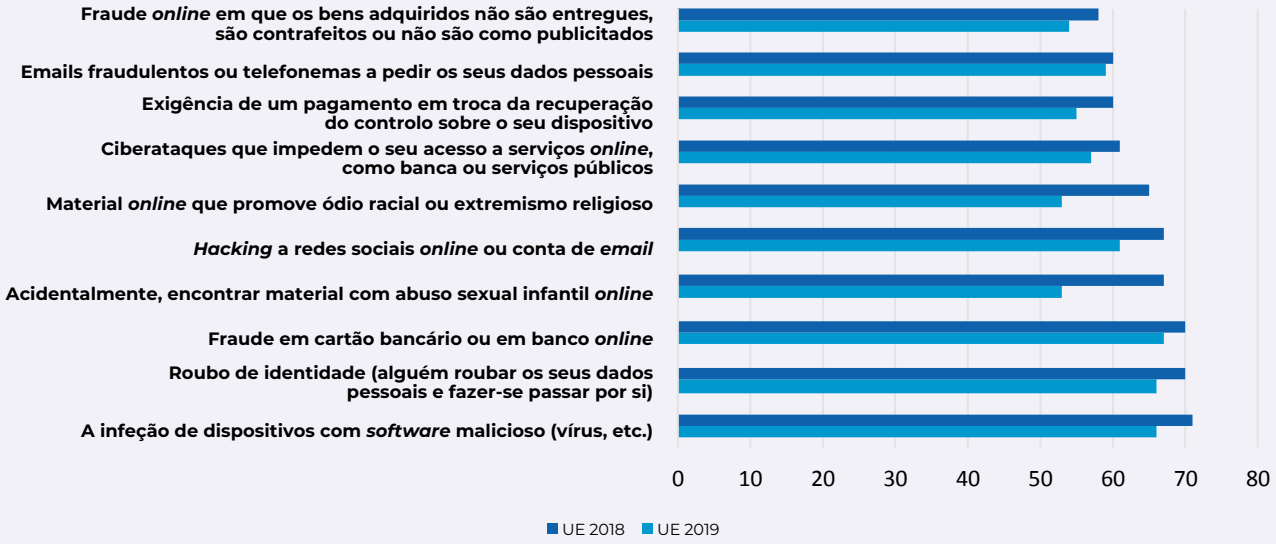


Figura 12 | Eurobarómetro 499 e 480

DESTAQUES

As preocupações dos indivíduos, em Portugal, aumentaram em quase todas as situações em causa, em contraciclo com a tendência de diminuição verificada na média da UE. Por exemplo, a preocupação com a fraude em cartão bancário ou em banco *online* aumentou 10 pp, para 74%, enquanto a média da UE desceu 3 pp, para 67%. A preocupação com o roubo de identidade, em Portugal, também aumentou significativamente, em 9 pp, para 77%, enquanto a média da UE diminuiu 4 pp, para 66%;

Esta tendência resulta em níveis de preocupação mais altos em Portugal do que a média da UE em relação a todas as situações apresentadas;

Em Portugal, as mulheres tendem a manifestar um pouco menos de preocupação do que os homens, bem como, de forma mais acentuada, os indivíduos com mais de 55 anos e aqueles que estudaram não mais do que até aos 15 anos de idade.

5. Nos últimos três anos, algum familiar, amigo ou conhecido dos indivíduos, em Portugal, experienciou ou foi vítima de alguma destas situações? (Múltiplas respostas possíveis) ***Utilizadores de Internet.*** **(%)***

	PT 2019	UE (tendência 2018-2019)	Tendência PT (2018-2019)
Descobrir software malicioso (vírus, etc.) no seu dispositivo	6	24 (-2)	-6
Roubo de identidade (alguém roubar os seus dados pessoais e fazer-se passar por si)	4	7 (=)	+1
Ser vítima de fraude em cartão bancário ou em banco online	2	11 (=)	-1
Acidentalmente, encontrar pornografia infantil online	1	3 (-1)	-2
Ocorrer hacking das suas redes sociais online ou conta de email	4	14 (=)	+1
Acidentalmente encontrar material online que promove ódio racial ou extremismo religioso	1	7 (-2)	-1
Ciberataques que impedem o seu acesso a serviços online, como banca ou serviços públicos	3	5 (-3)	=
Pedirem um pagamento em troca da recuperação do controlo sobre o seu dispositivo	2	6 (=)	+1
Receber emails fraudulentos ou telefonemas a pedir os seus dados pessoais (incluindo acesso ao computador, login, nformação de pagamentos ou bancária)	3	28 (+2)	=
Fraude online em que os bens adquiridos não são entregues, são contrafeitos ou não são como publicitados	4	15 (=)	-3
Outro cibercrime ou qualquer outro comportamento online ilegal (ciberataque, assédio ou bullying) [espontâneo]	4	4 (=)	+3
Não, nada [espontâneo]	50	33 (-4)	-5
Não sabe	34	21 (+12)	+14

*Esta pergunta é realizada pela primeira vez em 2018. Os dados apresentados no Eurobarómetro Especial 499 referem-se a todos os indivíduos. Contudo, em 2018, o Eurobarómetro Especial 480 refere-se somente a indivíduos utilizadores da Internet. Para efeitos de comparação, o Eurobarómetro Especial 499 apresenta também os dados referentes aos utilizadores de Internet. Optou-se por, neste ano, utilizar os dados comparáveis, isto é, apenas os referentes aos utilizadores de Internet.

Tabela 5 | Eurobarómetro 499 e 480

Aspetos sociodemográficos relevantes em Portugal, 2019

Sexo Os homens tendem a afirmar mais do que as mulheres que conhecem alguém que tenha experienciado ou sido vítima de uma das situações descritas: 20% dos homens e 13% das mulheres.

Idade Os indivíduos com idades compreendidas entre os 15 e os 24 anos tendem a afirmar mais que conhecem alguém que tenha experienciado ou sido vítima de uma das situações descritas, com 30%, enquanto as restantes faixas etárias apresentam números mais baixos. Por exemplo, apenas 13% das pessoas com mais de 55 anos responderam de forma afirmativa a esta questão.

Educação Os indivíduos que ainda estão a estudar tendem a afirmar mais que conhecem alguém que tenha experienciado ou sido vítima de uma das situações descritas, com 27%. Por exemplo, entre as pessoas que estudaram no máximo até aos 15 anos de idade, apenas 6% responderam afirmativamente a esta questão.

UE A média da UE coloca os homens e as mulheres com os mesmos valores quanto à questão apresentada, com 45% cada a identificarem pelo menos uma situação. Nos restantes itens verifica-se um alinhamento entre os valores de Portugal e a média da UE.

Nos últimos três anos, algum familiar, amigo ou conhecido dos indivíduos, em Portugal, experienciou ou foi vítima de alguma destas situações? (Múltiplas respostas possíveis) 2018-2019. *Utilizadores de Internet*. (%)

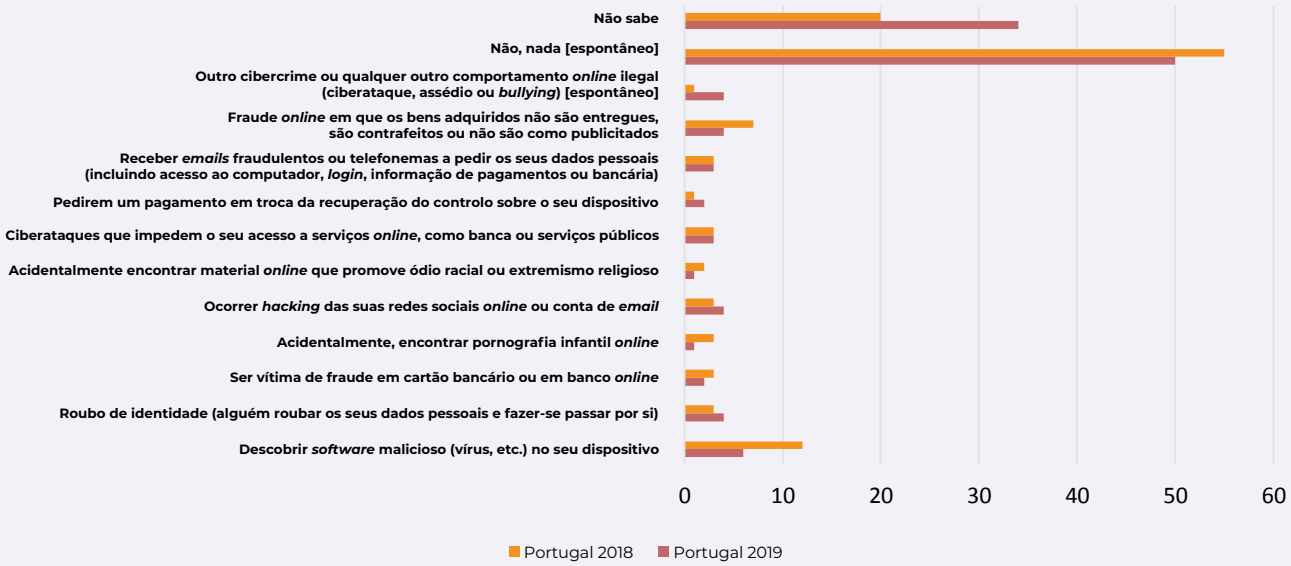


Figura 13 | Eurobarómetro 499 e 480

Nos últimos três anos, algum familiar, amigo ou conhecido dos indivíduos, em Portugal, experienciou ou foi vítima de alguma destas situações? (Múltiplas respostas possíveis) Comparação com UE. *Utilizadores de Internet*. (%)

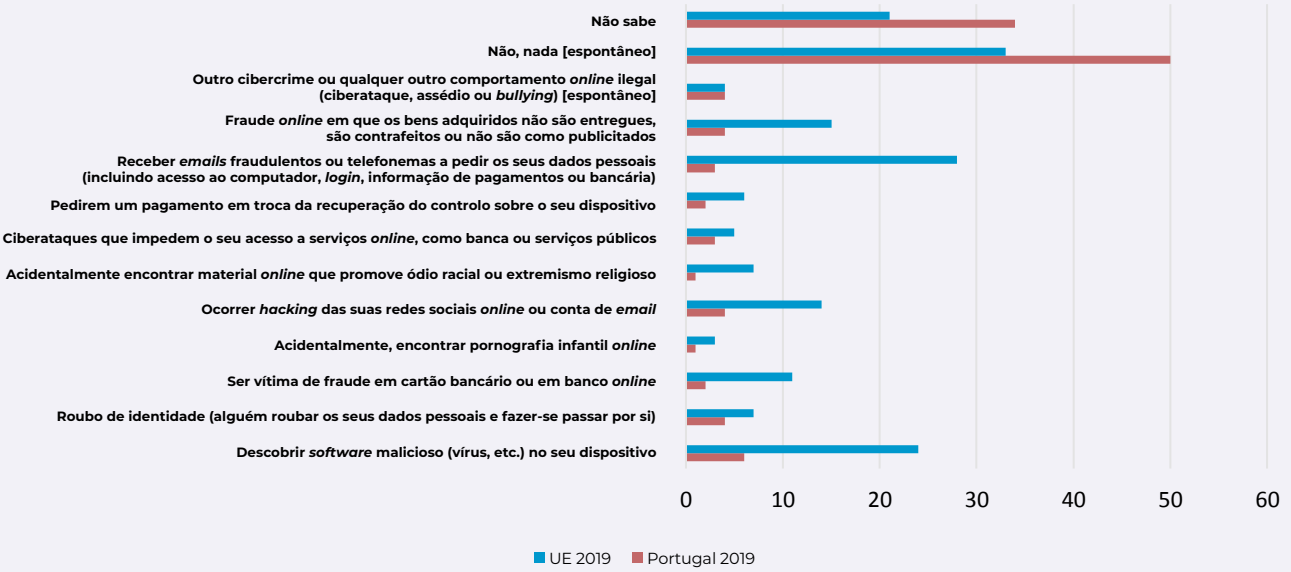


Figura 14 | Eurobarómetro 499

Nos últimos três anos, algum familiar, amigo ou conhecido dos europeus experienciou ou foi vítima de alguma destas situações? (Múltiplas respostas possíveis) 2018-2019. *Utilizadores de Internet*. (%)

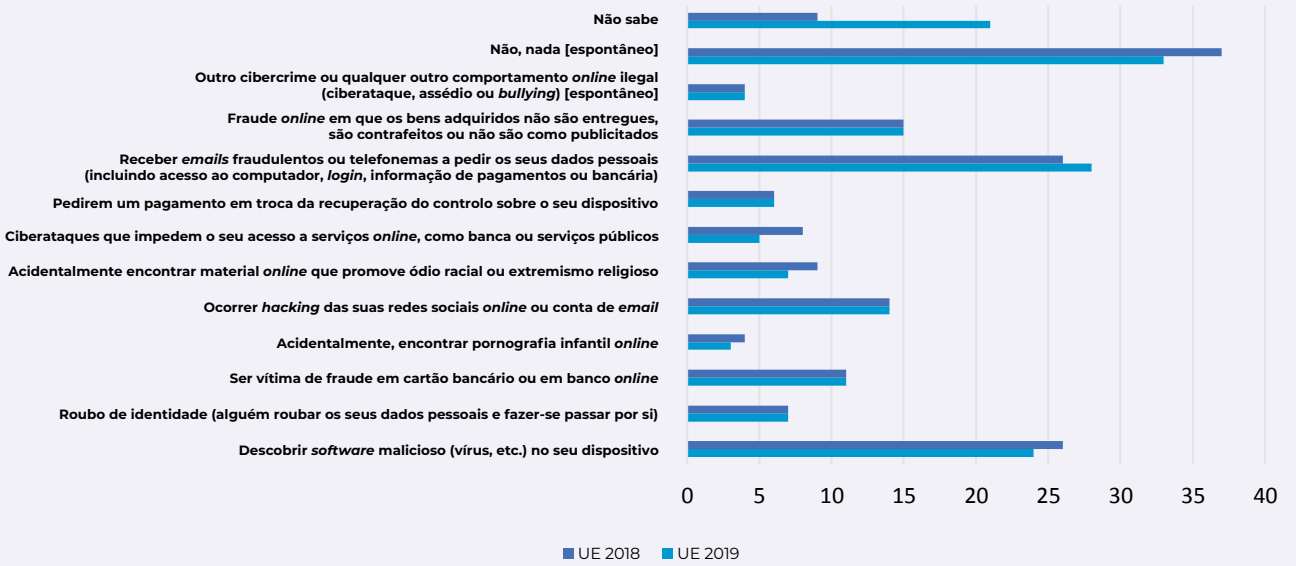


Figura 15 | Eurobarómetro 499 e 480

Destaques

Os indivíduos, em Portugal, em relação aos últimos três anos, afirmam menos do que a média da UE conhecer algum familiar, amigo ou conhecido que tenha experienciado ou sido vítima de alguma das situações descritas: 50% não conhecem e 34% não sabem (o que equivale a 16% a afirmarem que conhecem, menos 9 pp do que no ano anterior), enquanto a média da UE indica 33% que não conhecem e 21% que não sabem (isto é, 46% a afirmarem que conhecem);

A situação em relação à qual os indivíduos, em Portugal, mais afirmaram conhecer alguém que foi vítima ocorre no que respeita a descobrir *software* malicioso no seu dispositivo (6%). Contudo, a média da UE referente a esta situação é de 24%. A maior discrepância em relação à média da UE verifica-se no que diz respeito a conhecer alguém que tenha recebido *emails* fraudulentos ou telefonemas a pedir os dados pessoais, que apresenta 3% em Portugal e 28% na média da UE;

O perfil do indivíduo que mais conhece alguém que tenha sido vítima de uma das situações descritas, em Portugal, tende a ser homem, com idades compreendidas entre os 15 e os 24 anos e ainda estudante.

6. Consciência dos indivíduos, em Portugal, em relação à existência de um *website* ou de uma morada de *email* através dos quais se possa reportar um cibercrime ou qualquer outro comportamento ilegal *online* (ex.: ciberataques, assédio *online* ou *bullying*). (Múltiplas respostas possíveis) *Todos os utilizadores.* (%)*

	PT 2019	UE 2019
Sim, um website	11	12
Sim, um email	3	5
Sim, um formulário online	3	4
Sim, um número de contacto	4	6
Sim, outra forma de reportar um cibercrime ou qualquer outro comportamento ilegal online	4	4
Não, não tenho consciência da sua existência	80	77
Não sei	2	1
Total de "Tenho consciência da sua existência"	18	22

*O tipo de resposta possível alterou em relação ao Eurobarómetro 480.
Por isso, não se efetua uma comparação com o ano anterior.

Tabela 6 | Eurobarómetro 499

Aspetos sociodemográficos relevantes em Portugal, 2019

Sexo Os homens assumem ligeiramente mais, com 19%, do que as mulheres, com 17%, terem consciência de algum destes meios de reporte de cibercrimes ou de qualquer outro comportamento ilegal *online*.

Idade Apenas 5% dos indivíduos com mais de 55 anos de idade referem ter consciência de algum destes meios, enquanto, por exemplo, entre os que têm idades entre os 25 e os 39 anos, o valor atinge os 33%.

Educação Os indivíduos que estudaram no máximo até aos 15 anos de idade tendem a conhecer menos qualquer destes meios do que os outros. Por exemplo, apenas 6% afirmaram conhecer algum destes meios, enquanto, entre as pessoas que estudaram até depois dos 20 anos de idade, o valor é de 42%.

UE Tendências genericamente alinhadas com a média da UE.

Eurobarómetro 499

Consciência dos indivíduos, em Portugal, em relação à existência de um *website* ou de uma morada de *email* através dos quais se possa reportar um cibercrime ou qualquer outro comportamento ilegal *online*. (Múltiplas respostas possíveis) 2019. *Todos os utilizadores*. (%)

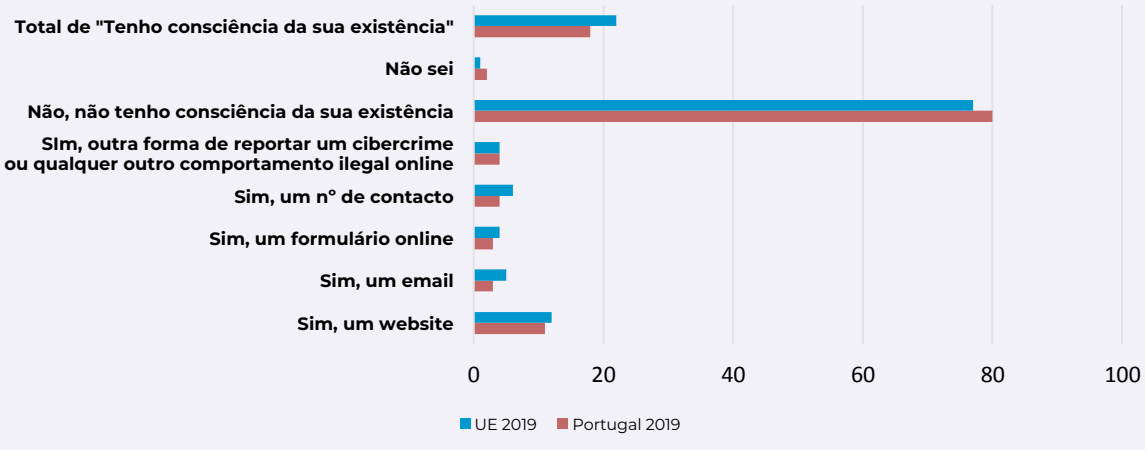


Figura 16 | Eurobarómetro 499

Destaques

Baixa percentagem de indivíduos (18%), em Portugal, que conhecem qualquer um dos meios referidos, através dos quais se possa reportar um cibercrime ou qualquer outro comportamento ilegal *online*. A média da UE a este respeito também é baixa, mas menos (22%);

O meio mais conhecido para o efeito, entre os indivíduos em Portugal e na média da UE, é o *website* – 11% e 12%, respetivamente.

7. Independentemente de terem sido ou não vítimas de um cibercrime, o que fariam os indivíduos, em Portugal, se experienciassem ou fossem vítimas das seguintes situações? (Múltiplas respostas possíveis) Pelo menos uma ação e a mais frequente.
Todos os utilizadores. **(%)***

	PT 2019	Ação + frequente PT/UE 2019	UE (tendência 2018-2019)	Tendência PT (2018-2019)
Descobrir software malicioso (vírus, etc.) no seu dispositivo	71	Cont. polícia 40/23	70 (+2)	-1
Roubo de identidade (alguém roubar os seus dados pessoais e fazer-se passar por si)	79	Cont. polícia 66/72	86 (-1)	-3
Ser vítima de fraude em cartão bancário ou em banco online	78	Cont. polícia 69/67	86 (-2)	-4
Acidentalmente, encontrar pornografia infantil online	77	Cont. polícia 56/66	82 (+1)	+4
Ocorrer hacking das suas redes sociais online ou conta de email	73	Cont. polícia 42/36	78 (+1)	+2
Acidentalmente encontrar material online que promove ódio racial ou extremismo religioso	72	Cont. polícia 49/53	74 (+4)	+13
Ciberataques que impedem o seu acesso a serviços online, como banca ou serviços públicos	73	Cont. polícia 46/40	79 (+3)	+10
Pedirem um pagamento em troca da recuperação do controlo sobre o seu dispositivo	76	Cont. polícia 61/60	80 (+1)	-1
Receber emails fraudulentos ou telefonemas a pedir os seus dados pessoais (incluindo acesso ao computador, login, informação de pagamentos ou bancária)	72	Cont. polícia 46/38	67 (+3)	+16
Fraude online em que os bens adquiridos não são entregues, são contrafeitos ou não são como publicitados	75	Cont. polícia 48/43	84 (+2)	-2

* Apenas se comparam os anos de 2018 e 2019 porque nos inquéritos anteriores somente se apresentam dados respeitantes a utilizadores de Internet, além de ter ocorrido uma alteração na formulação da pergunta que se considera relevante.

Tabela 7 | Eurobarómetro 499 e 480

Situação com mais reação por cada resposta possível

	Situação com mais reação PT 2019	Valores PT 2019	Situação com mais reação UE 2019	Valores UE 2019
Nada	*Descobrir software malicioso… e emails fraudulentos…*	10	*Receber emails fraudulentos…*	24
Contactava a polícia	*Ser vítima de fraude em cartão bancário…*	69	*Roubo de identidade…*	72
Contactava o website/vendedor	*Fraude online em que os bens adquiridos…*	33	*Fraude online em que os bens adquiridos…*	34
Contactava o prestador do serviço de internet	*Descobrir software malicioso…e hacking das redes sociais…*	13	*Descobrir software malicioso…*	18
Contactava uma organização de proteção do consumidor	*Fraude online em que os bens adquiridos…*	10	*Fraude online em que os bens adquiridos…e receber emails fraudulentos…*	11
Reportava a situação através de um website ou email oficial (outro que não o da polícia)	*Receber emails fraudulentos…*	5	*Ciberataques que impedem o seu acesso a serviços online…e receber emails fraudulentos…*	6
Outro [espontânea]	*Descobrir software malicioso…*	15	*Descobrir software malicioso…*	13
Não sei	*Descobrir software malicioso…e material online que promove ódio*	19	*Descobrir software malicioso…*	11

Tabela 8 | Eurobarómetro 499 e 480

Aspetos sociodemográficos relevantes em Portugal, 2019

Sexo Os homens tendem a pretender agir mais do que as mulheres em qualquer das situações descritas. Por exemplo, 78% dos homens afirmam que agiriam de algum modo contra a fraude *online* em que os bens adquiridos não são entregues, são contrafeitos ou não se apresentam como foram publicitados, enquanto apenas 71% das mulheres afirmam o mesmo.

Idade Os indivíduos com mais do que 55 anos de idade tendem a afirmar menos do que os das restantes faixas etárias que agiriam em qualquer uma das situações. Por exemplo, 56% das pessoas com mais de 55 anos afirmam que agiriam de algum modo quanto a, acidentalmente, encontrar pornografia infantil *online*, enquanto entre as pessoas com idades compreendidas entre os 15 e os 24 anos o valor atinge os 94%.

Educação Os indivíduos com mais estudos ou que ainda estudam tendem a pretender agir mais em qualquer das situações. Por exemplo, 53% das pessoas que estudaram até aos 15 anos de idade no máximo afirmam que agiriam no caso de *hacking* das suas redes sociais *online* ou conta de *email*, enquanto 87% das pessoas que estudaram até depois dos 20 anos de idade o afirmam também.

UE Tendências semelhantes, embora na média da UE se verifique, em geral, menor contraste entre grupos do que em Portugal.

Eurobarómetro 499

Independentemente de terem sido ou não vítimas de um cibercrime, o que fariam os indivíduos, em Portugal, se experienciassem ou fossem vítimas das seguintes situações?
(Múltiplas respostas possíveis) Pelo menos uma ação. 2018-2019. *Todos os utilizadores.* (%)

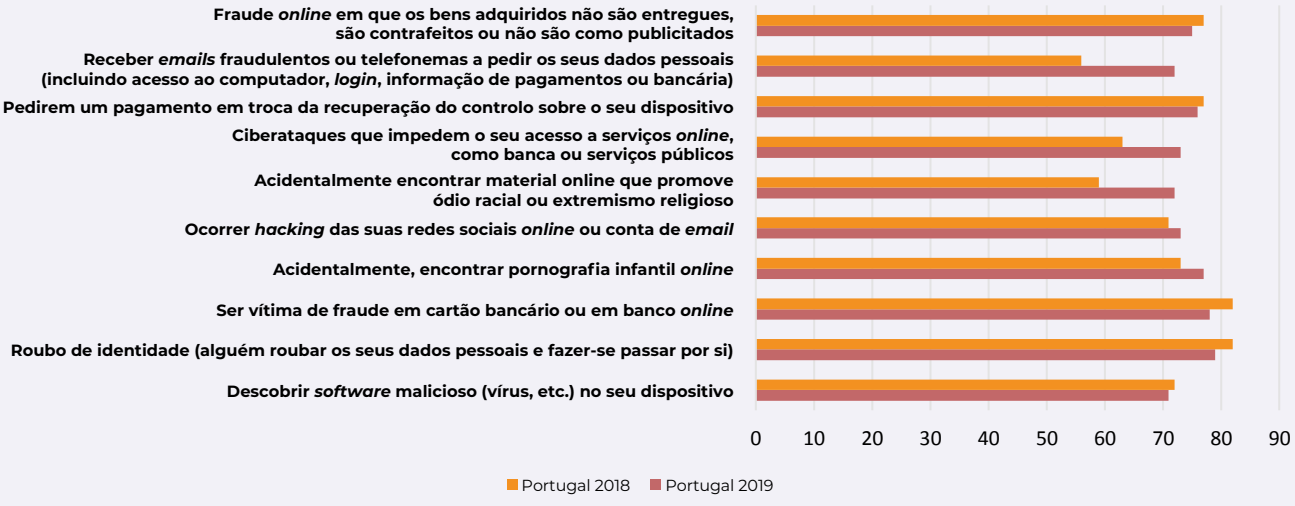


Figura 17 | Eurobarómetro 499 e 480

Independentemente de terem sido ou não vítimas de um cibercrime, o que fariam os indivíduos, em Portugal, se experienciassem ou fossem vítimas das seguintes situações?
(Múltiplas respostas possíveis) Pelo menos uma ação. Comparação com UE. *Todos os utilizadores.* (%)

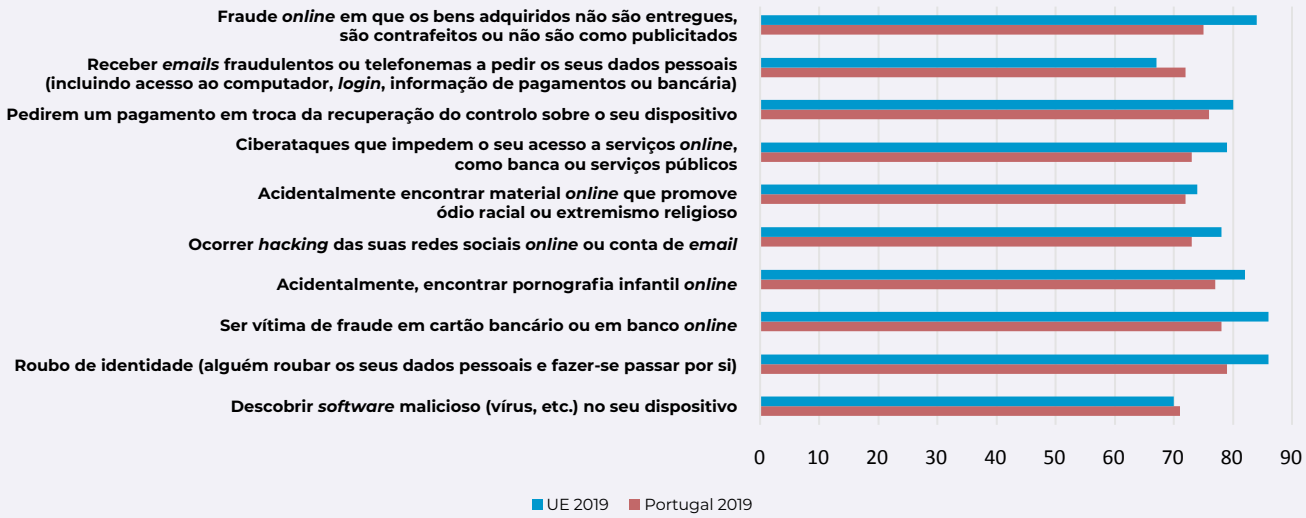


Figura 18 | Eurobarómetro 499

Independentemente de terem sido ou não vítimas de um cibercrime, o que fariam os europeus se experienciassem ou fossem vítimas das seguintes situações? (Múltiplas respostas possíveis). Pelo menos uma ação. 2018 2019. *Todos os utilizadores.* (%)

Figura 19 | Eurobarómetro 499 e 480

Destaques

O roubo de identidade é o tipo de situação em relação à qual os indivíduos, em Portugal, mais afirmam que reagiriam de alguma forma caso fossem vítimas, com 79%;

A ação que os indivíduos, em Portugal, mais afirmam que realizariam caso lhes acontecesse alguma das situações apresentadas seria contactar a polícia, tratando-se da resposta mais frequente em relação a todas as situações. O mesmo se verifica na média da UE. A situação que mais se destaca, em Portugal, com esta resposta é a que diz respeito a ser vítima de fraude em cartão bancário ou em banco *online*, com 69%. Na média da UE a situação que mais se destaca com esta resposta é o roubo de identidade, com 72%;

Em relação ao ano anterior, existem várias subidas, mas receber *emails* fraudulentos ou telefonemas a pedir os seus dados pessoais é a situação que mais vê subir a disponibilidade para agir, em 16 pp;

A média da UE é quase sempre superior a Portugal na disponibilidade para reagir;

Algumas situações, apesar de maioritariamente conduzirem ao contacto com a polícia, como no que se refere à fraude *online* em que os bens adquiridos não são entregues, são contrafeitos ou não são como publicitados, o contacto com o *website*/vendedor tem importância, com 33% de resposta entre os indivíduos em Portugal e 34% na média da UE;

A situação que mais respostas "não sei" provocou, quer em Portugal, quer na média da UE, é a respeitante a descobrir *software* malicioso, com 19% e 11%, respetivamente. Em Portugal, acidentalmente, encontrar material *online* que promove ódio racial ou extremismo religioso, também obteve 19% de respostas "não sei".

Síntese - As Atitudes dos indivíduos, em Portugal, face à Cibersegurança

Há mais indivíduos, utilizadores de Internet, sem nenhuma preocupação em relação a atividades como o banco *online* ou a compra de bens e serviços *online* do que na média da UE.

Todavia, estes mesmos indivíduos preocupam-se mais do que a média da UE com o uso indevido dos dados pessoais em atividades deste tipo.

Em relação ao ano anterior, há menos indivíduos, utilizadores de Internet, em 2019, com medo de não receber os produtos ou serviços comprados *online*.

Os indivíduos sentem-se menos informados em relação ao risco de cibercrime do que a média da UE.

Os homens, os jovens e as pessoas com mais formação académica tendem a sentir-se mais bem informados.

Há menos indivíduos em 2019 a sentirem-se capazes de se proteger o suficiente contra o cibercrime do que no ano anterior.

As preocupações dos indivíduos, utilizadores de Internet, com a possibilidade de virem a ser vítimas de cibercrimes aumentou em 2019 em relação ao ano anterior e é maior do que a média da UE.

Os indivíduos, utilizadores de Internet, conhecem menos pessoas vítimas de cibercrime do que a média da UE.

Grande parte dos indivíduos desconhece qualquer meio através do qual possam reportar um cibercrime ou qualquer outro comportamento ilegal *online*.

O contacto com a polícia é a reação que mais indivíduos escolheriam na eventualidade de serem vítimas de ciberameaças.

CNCS
Centro Nacional de Cibersegurança PORTUGAL

G. — COMPORTAMENTOS

Observatório de **Cibersegurança**

Os comportamentos são uma vertente muito importante das boas práticas de ciber-higiene, na medida em que é através da ação que ocorre uma efetiva proteção do próprio e dos outros no uso das TIC. Este capítulo é subdividido em indicadores de comportamento respeitantes aos Indivíduos e às Organizações (Empresas, Administração Pública Central e Regional e Câmaras Municipais). Recorre em parte ao referido Eurobarómetro especial 499, mas também, e em grande medida, a dados fornecidos pelo Eurostat e pela DGEEC.

COMPORTAMENTOS INDIVIDUAIS

No âmbito dos comportamentos individuais, o Eurobarómetro especial 499 continua a ser um documento relevante. A partir desta fonte, é possível ter acesso a indicadores sobre mudanças de comportamento fruto de preocupações (isto é, de atitudes), cuidados com as *passwords*, reconhecimento de que se foi vítima ou a capacidade de reação ao cibercrime.

8. As preocupações dos indivíduos, em Portugal, com a Internet fizeram alterar o seu comportamento em alguma das seguintes formas? (Múltiplas respostas possíveis) ***Utilizadores de Internet.*** **(%)**

	PT 2019	UE (tendência 2018-2019)	Tendência PT (2018-2019)	Tendência PT* (2014-2018)	Tendência PT (2013-2014)
Instalou um software antivírus	35	42 (-5)	-9	-6	+26
Não abre emails de pessoas desconhecidas	43	42(-3)	-1	+3	+18
É menos provável fornecer informação pessoal a websites	33	30 (-7)	-1	=	+3
Só utiliza o seu próprio computador	26	32 (-2)	+3	-7	+15
Só visita websites que conhece e nos quais confia	34	32 (=)	+4	+1	+11
Utiliza passwords diferentes para diferentes websites	20	29 (=)	+7	-13	+11
Utiliza passwords mais complexas do que no passado	15	26 (-1)	+3	**	**
Altera as suas passwords regularmente	14	21 (=)	-2	-11	**
Alterou as definições de segurança (ex.: no browser, na rede social online)	10	13 (-4)	+1	-6	+3
É menos provável comprar bens e serviços online	12	10 (-1)	-5	-8	-13
Cancelou uma compra online devido a suspeitas em relação ao vendedor ou ao website	2	9 (-1)	-3	-1	+5
É menos provável usar o banco online	11	8 (-1)	-2	-11	-2
Usa um gestor de passwords	3	7	**	**	**
Usa características biométricas (p. ex.: reconhecimento facial, impressões digitais)	4	13	**	**	**
Não se liga à Internet através de hotspots inseguros	15	23	**	**	**
Outra [espontâneo]	6	8 (+5)	+4	+1	=
Nenhuma/Não está preocupado com a segurança online [espontâneo]	13	4 (-11)	-4	+4	-10
Não sabe	1	3 (+1)	=	**	+1

* Não se estabelece uma comparação com 2017 porque os dados desse ano são recolhidos no âmbito do Eurobarómetro 460 *Attitudes towards the impact of digitisation and automation on daily life*. Sendo uma base estatística semelhante, não é a mesma.
** Opções de resposta não disponíveis nesses anos.

Tabela 9 | Eurobarómetro 499, 480, 423 e 404

Aspetos sociodemográficos relevantes em Portugal, 2019

Sexo As mulheres tendem a identificar mais ações e a sentir mais preocupação do que os homens, com 87% e 85%, respetivamente.

Idade Os indivíduos com mais de 55 anos tendem a identificar mais ações e a sentir mais preocupação do que as restantes faixas etárias. Por exemplo, enquanto os indivíduos com mais de 55 anos apresentam o valor de 88%, os indivíduos com idades compreendidas entre os 15 e os 24 anos apresentam 80%.

Educação Os indivíduos que estudaram até depois dos 20 anos de idade têm valores contrastantes com aqueles que ainda estudam, com 94% a identificarem ações e a sentir preocupação, enquanto os que ainda estudam apenas chegam aos 79%.

UE A média da UE tende, em geral, a apresentar menos divergências entre os grupos.

As preocupações dos indivíduos, em Portugal, com a Internet fizeram alterar o seu comportamento em alguma das seguintes formas? (Múltipla respostas possíveis) 2013-2019. *Utilizadores de Internet*. (%)

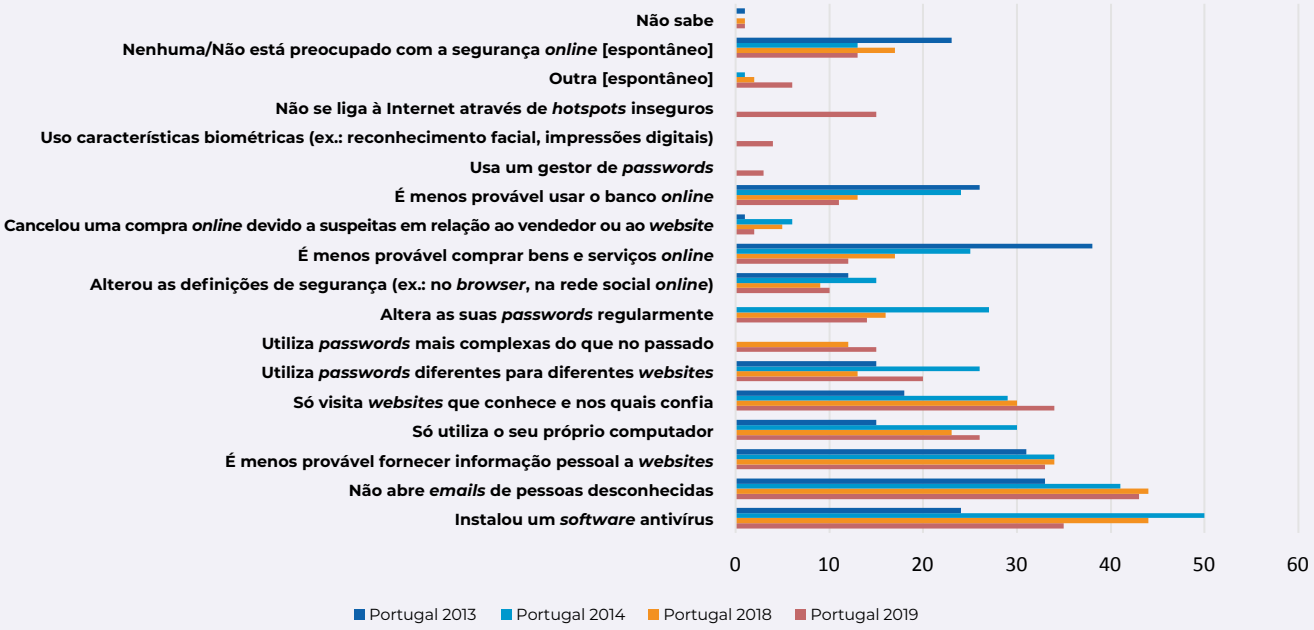


Figura 20 | Eurobarómetro 499, 480, 423 e 404

As preocupações dos indivíduos, em Portugal, com a Internet fizeram alterar o seu comportamento em alguma das seguintes formas? (Múltipla respostas possíveis) Comparação com UE. *Utilizadores de Internet*. (%)

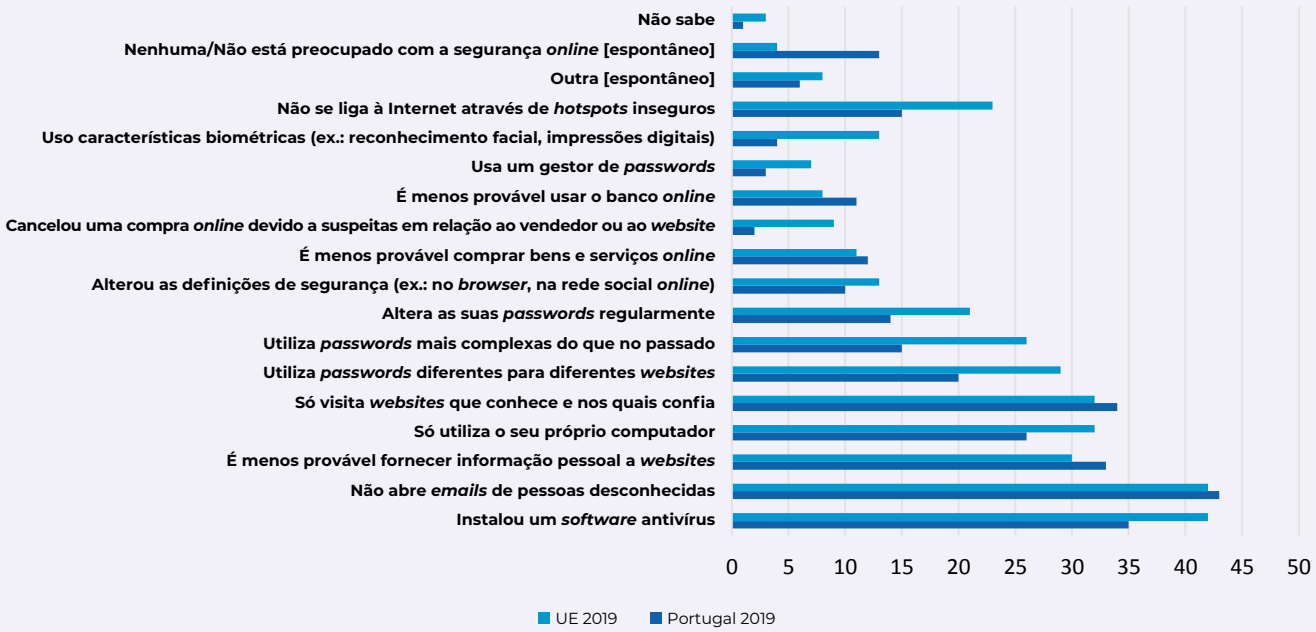


Figura 21 | Eurobarómetro 499

As preocupações dos indivíduos, em Portugal, com a Internet fizeram alterar o seu comportamento em alguma das seguintes formas? (Múltipla respostas possíveis) 2018-2019. *Utilizadores de Internet.* (%)

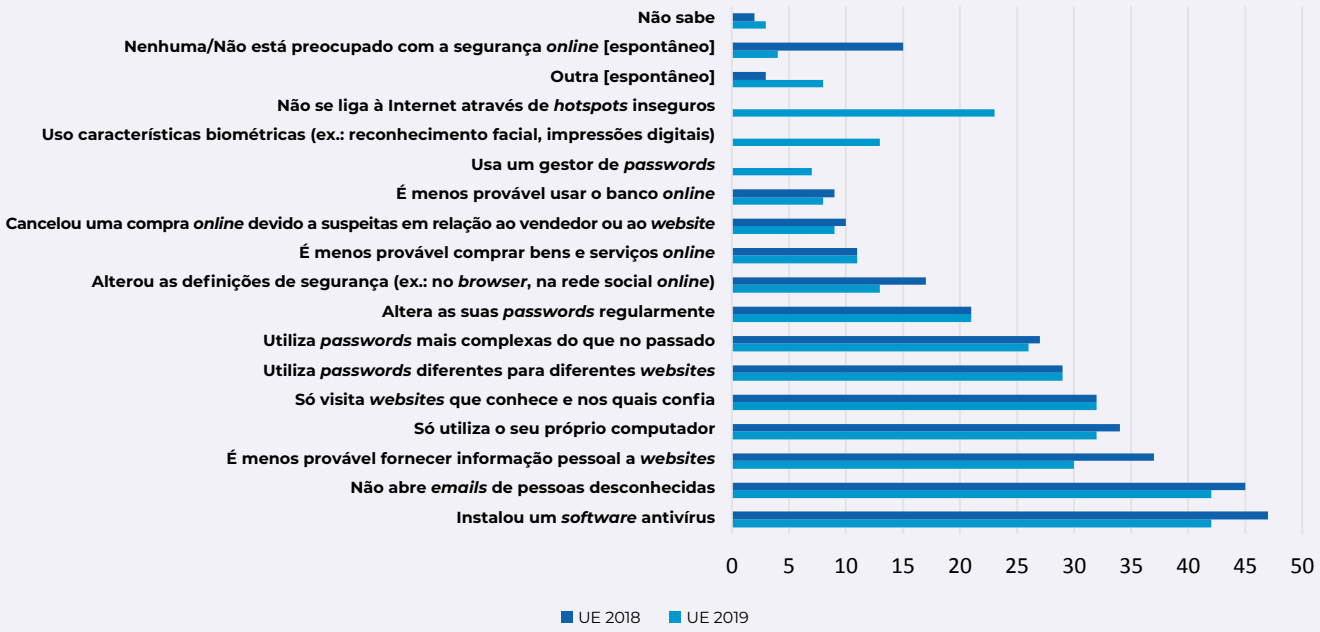


Figura 22 | Eurobarómetro 499 e 480

Destaques

O comportamento mais frequente entre os indivíduos, em Portugal, em resultado de preocupações com a Internet é o de não abrirem *emails* de pessoas desconhecidas, que regista o valor de 43%. A média da UE é de 42%, também o comportamento mais frequente, mas com igual percentagem do que a instalação de um *software* antivírus;

A maior descida em relação a 2018, entre os indivíduos, em Portugal, diz respeito a instalar *software* antivírus, em menos 9 pp (para 35%). A maior subida, de 7 pp (para 20%), corresponde à utilização de *passwords* diferentes para diferentes *websites* – todavia, os indivíduos, em Portugal, continuam a ter menos cuidados com as *passwords* do que a média da UE. No somatório, há uma ligeira subida no que diz respeito a pessoas que alteram o seu comportamento, em Portugal, em 4 pp (subtraindo os que referem "nenhuma" ou "não sabe");

Identifica-se ainda uma discrepância relevante entre os números em Portugal e a média da UE nos novos indicadores, em particular no uso de características biométricas, que em Portugal atinge os 4% e a média da UE é de 13%;

Em termos sociodemográficos, em Portugal, as mulheres, os indivíduos com mais de 55 anos e aqueles que estudaram até depois dos 20 anos de idade tendem a afirmar mais do que os restantes agir em resultado de preocupações com a Internet.

9. Para qual destes serviços *online*, se algum, os indivíduos, em Portugal, alteraram a *password* que usam para aceder às suas contas, nos últimos 12 meses? (Múltiplas respostas possíveis) *Utilizadores de Internet*. (%)

	PT 2019	UE (tendência 2017-2018)	Tendência PT (2018-2019)	Tendência PT (2017-2018)	Tendência PT (2014-2017)	Tendência PT (2013-2014)
Email	25	37 (+3)	+4	-13	-7	+12
Banco online	15	30 (+4)	=	=	-14	+21
Redes sociais online	16	25 (-1)	-4	-8	+2	-3
Websites de compras	6	16 (+1)	-5	+6	-5	+4
Websites de serviços públicos	6	9 (+1)	-1	-1	-2	*
Jogos online	3	7 (+1)	+1	=	-5	*
Outra [espontâneo]	7	10 (+5)	+6	-3	+2	*
Nenhum [espontâneo]	48	31 (-9)	-11	+6	+14	-18
Não sabe	21	11 (+8)	+20	=	=	=
Total "Mudou a password"	41	69 (+11)	+1	-2	-18	+18

*A pergunta não foi realizada nestes anos. Devido ao menor número de opções, isso pode interferir na comparabilidade dos resultados.

Tabela 10 | Eurobarómetro 499, 480, 464a, 423 e 404

Aspetos sociodemográficos relevantes em Portugal, 2019

Sexo Os homens tendem a mudar mais as *passwords* do que as mulheres: 45% mudaram alguma das *passwords*, contra 37% das mulheres.

Idade Os indivíduos com idades compreendidas entre os 40 e os 54 anos de idade tendem a mudar mais alguma das *passwords* do que as restantes faixas etárias, atingindo os 48%. Os indivíduos com mais de 55 anos, por exemplo, apenas atingem os 35%.

Educação Os indivíduos que estudaram até depois dos 20 anos de idade afirmam mais do que os restantes que mudaram alguma das *passwords* identificadas, apresentando o valor de 63%. Os que estudaram no máximo até aos 15 anos de idade atingem apenas os 26%.

UE Em relação à idade, a média da UE apresenta valores mais altos na faixa etária entre os 25 e os 39 anos, com 77% a terem alterado alguma *password*. Em relação ao nível educacional, as pessoas que ainda estudam destacam-se na média da UE, com 76% a identificarem alguma mudança de *password*.

Eurobarómetro 499

Para qual destes serviços *online*, se algum, indivíduos, em Portugal, alteraram a *password* que usam para aceder às suas contas, nos últimos 12 meses? (Múltiplas respostas possíveis) 2013-2019. *Utilizadores de Internet.* (%)

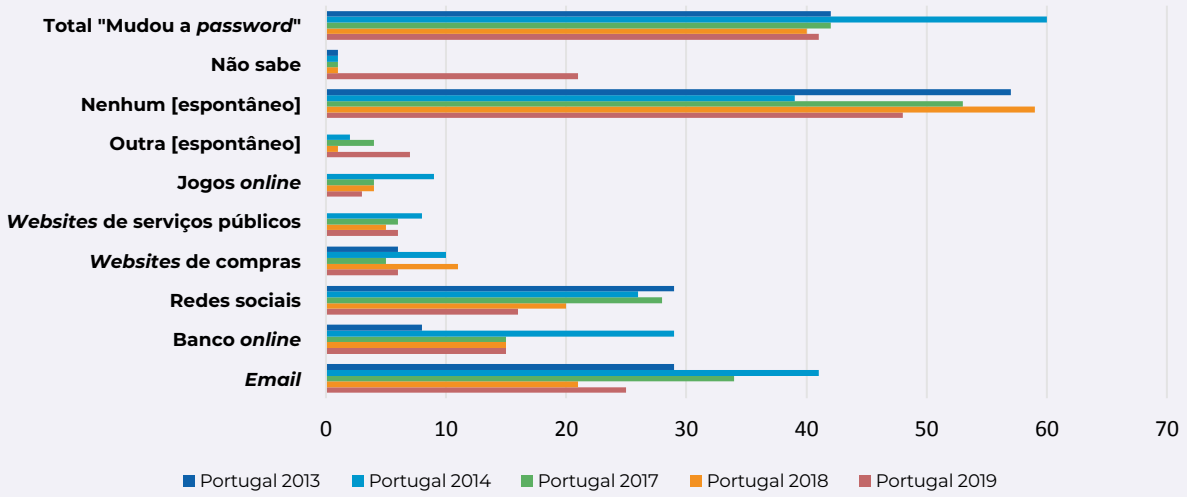


Figura 23 | Eurobarómetro 499, 480, 464a, 423 e 404

Para qual destes serviços *online*, se algum, os indivíduos, em Portugal, alteraram a *password* que usam para aceder às suas contas, nos últimos 12 meses? (Múltipla respostas possíveis) Comparação com UE. *Utilizadores de Internet.* (%)

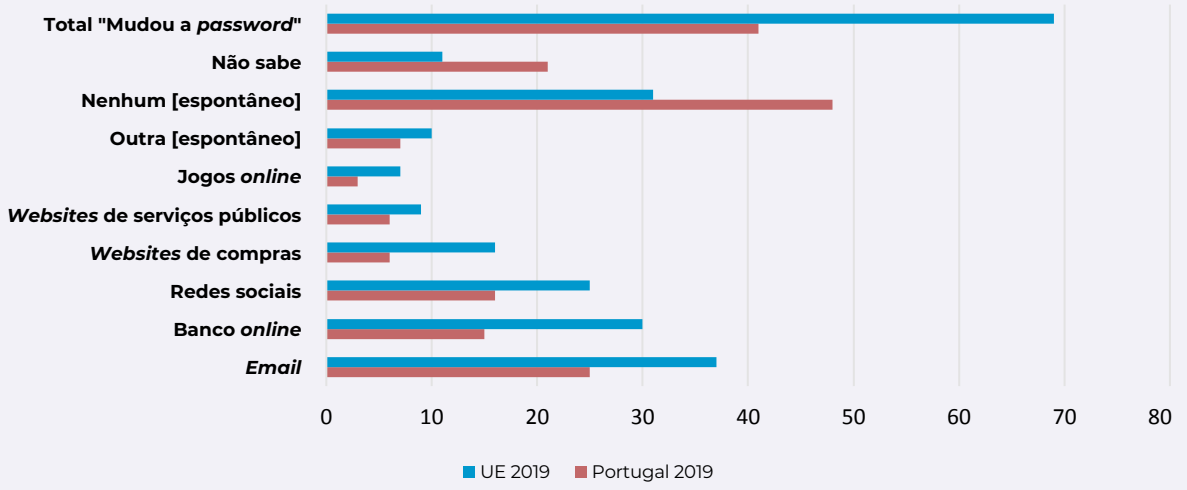


Figura 24 | Eurobarómetro 499

Para qual destes serviços *online*, se algum, os europeus alteraram a *password* que usam para aceder às suas contas, nos últimos 12 meses? (Múltipla respostas possíveis) 2018-2019. *Utilizadores de Internet*. (%)

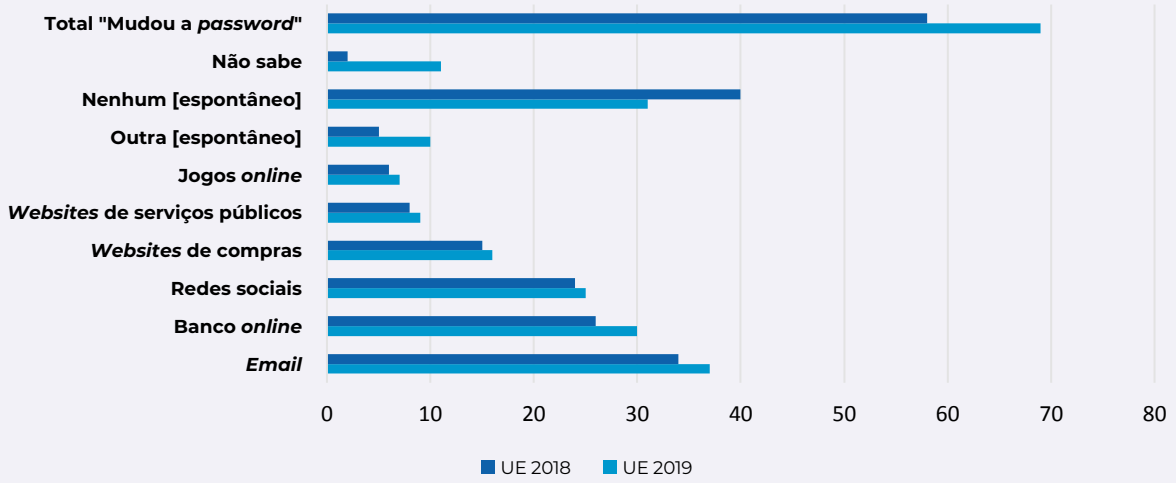


Figura 25 | Eurobarómetro 499 e 480

DESTAQUES

Os indivíduos, em Portugal, mudaram menos as suas *passwords* nos 12 meses anteriores do que a média da UE, com 48% a não terem mudado qualquer *password*, enquanto a média da UE a este respeito fica pelos 31%;

A média da UE é sempre superior aos números em Portugal em termos de mudança de *passwords* em qualquer das plataformas indicadas;

Em relação ao ano anterior, há uma diminuição em 11 pp de indivíduos, em Portugal, que afirmam que não mudaram nenhuma *password*; contudo, há um aumento em 20 pp de indivíduos que respondem que não sabem;

Em Portugal, o total de pelo menos uma mudança de *password* aumentou apenas 1 pp em relação ao ano de 2018, para 41%, quando a média da UE é de 69% e aumentou 11 pp;

O *email*, com 25% (mais 4 pp do que no ano anterior), é o tipo de conta em relação à qual se verificam mais mudanças de *password*, em Portugal. O mesmo ocorre no âmbito da média da UE, com 37% (mais 3 pp do que no ano anterior);

As contas de redes sociais e dos bancos *online* são as que, logo a seguir ao *email*, mais mudanças de *password* apresentam entre os indivíduos, com 16% e 15%, respetivamente.

10. Nos últimos três anos, com que frequência os indivíduos, em Portugal, experienciaram pessoalmente ou foram vítimas de cada uma das seguintes situações? Pelo menos uma vez. ***Utilizadores de Internet.*** **(%)**

	PT 2019	UE (tendência 2018-2019)	Tendência PT (2018-2019)
Descobrir software malicioso (vírus, etc.) no seu dispositivo	11	28 (-5)	-13
Roubo de identidade (alguém roubar os seus dados pessoais e fazer-se passar por si)	1	6 (-1)	-4
Ser vítima de fraude em cartão bancário ou em banco online	2	8 (-2)	-4
Acidentalmente, encontrar pornografia infantil online	2	5 (-2)	-4
Ocorrer hacking das suas redes sociais online ou conta de email	3	11 (-1)	-4
Acidentalmente encontrar material online que promove ódio racial ou extremismo religioso	3	13 (-5)	-4
Ciberataques que impedem o seu acesso a serviços online, como banca ou serviços públicos	2	8 (-1)	-6
Pedirem um pagamento em troca da recuperação do controlo sobre o seu dispositivo	2	8 (-1)	-5
Receber emails fraudulentos ou telefonemas a pedir os seus dados pessoais (incluindo acesso ao computador, login, informação de pagamentos ou bancária)	5	36 (+2)	-5
Fraude online em que os bens adquiridos não são entregues, são contrafeitos ou não são como publicitados	3	12 (-3)	-4

Tabela 11 | Eurobarómetro 499 e 480

Aspetos sociodemográficos relevantes em Portugal, 2019

Sexo | Idade | Educação Dada a base da amostra e a irregularidade das diferenças, não se consideram relevantes as possíveis tendências identificadas.

UE Na média da UE, a única diferença entre grupos considerada relevante é a que ocorre entre sexos, em que os homens tendem a reconhecer mais do que as mulheres já terem sido vítimas de alguma destas situações. Por exemplo, na média da UE, 31% dos homens reconhecem ter sido vítimas de *software* malicioso, enquanto apenas 24% das mulheres o fazem.

Eurobarómetro 499

Nos últimos três anos, com que frequência os indivíduos, em Portugal, experienciaram pessoalmente ou foram vítimas de cada uma das seguintes situações? Pelo menos uma vez. 2018-2019.
Utilizadores de Internet. (%)

Figura 26 | Eurobarómetro 499 e 480

Nos últimos três anos, com que frequência os indivíduos, em Portugal, experienciaram pessoalmente ou foram vítimas de cada uma das seguintes situações? Pelo menos uma vez. Comparação com UE.
Utilizadores de Internet. (%)

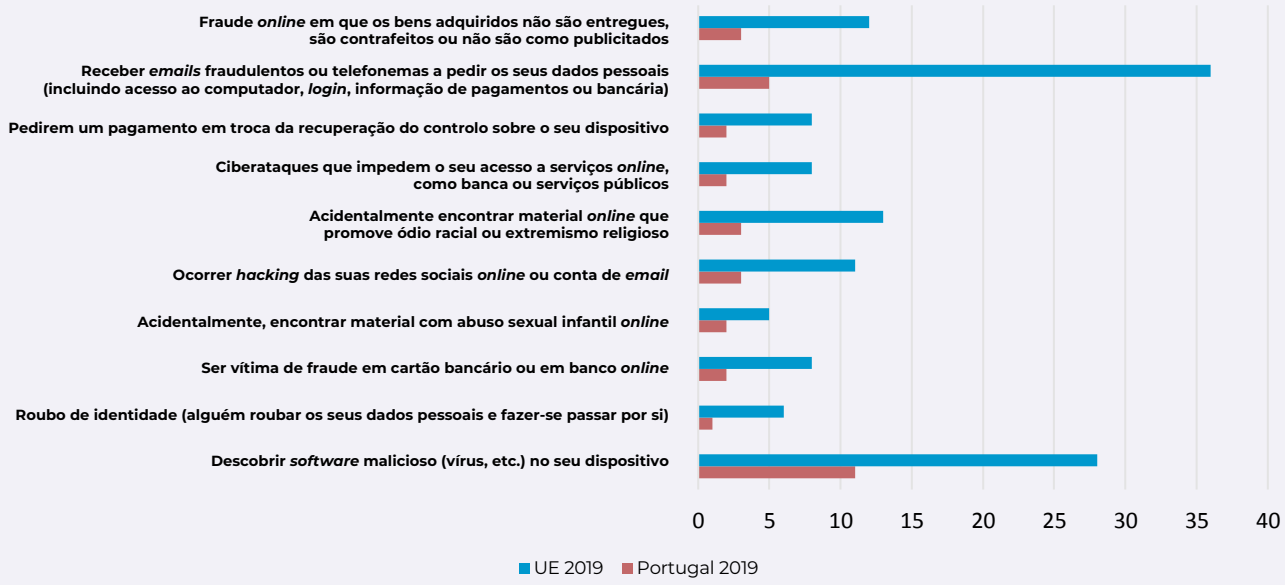


Figura 27 | Eurobarómetro 499

Nos últimos três anos, com que frequência os europeus experienciaram pessoalmente ou foram vítimas de cada uma das seguintes situações? Pelo menos uma vez. *Utilizadores de Internet.* (%)

Figura 28 | Eurobarómetro 499 e 480

DESTAQUES

Os indivíduos, em Portugal, reconhecem menos do que a média da UE como tendo experienciado ou sido vítimas de qualquer uma das situações descritas. As maiores discrepâncias com a média da UE ocorrem em relação a receber *emails* fraudulentos ou telefonemas a pedir os seus dados pessoais, com 5% entre os indivíduos em Portugal e 36% na média da UE, e quanto a descobrir *software* malicioso, com 11% em Portugal e 28% na média da UE – não obstante estas discrepâncias, ambas as situações são as mais identificadas entre os indivíduos em Portugal e na média da UE;

Em relação a 2018, em Portugal, a situação que mostra maior alteração é a que diz respeito a descobrir *software* malicioso, com menos 13 pp;

Verifica-se uma diminuição em relação ao ano anterior em todas as situações identificadas pelos indivíduos em Portugal. O mesmo se passa na média da UE, com exceção de receber *emails* fraudulentos ou telefonemas a pedir os seus dados pessoais, que cresce 2 pp.

11. O que fizeram os indivíduos, em Portugal, em cada uma das seguintes situações experienciadas pessoalmente ou de que foram vítimas? (Múltiplas respostas possíveis) Pelo menos uma ação e a mais frequente. *Vítimas*. * (%)

	PT 2019	Ação + frequente PT/UE 2019	UE (tendência 2018-2019)	Tendência PT (2018-2019)
Descobrir software malicioso (vírus, etc.) no seu dispositivo	65	Outro 47/ Nada 43	52 (-2)	-18
Roubo de identidade (alguém roubar os seus dados pessoais e fazer-se passar por si)	63	Nada 37/ Cont. polícia 28	74 (+3)	+19
Ser vítima de fraude em cartão bancário ou em banco online	81	Outro 29/ Cont. vend. 35	84 (+1)	+21
Acidentalmente, encontrar pornografia infantil online	50	Nada 35/34	61 (+7)	-13
Ocorrer hacking das suas redes sociais online ou conta de email	84	Cont. vend. 27/ Nada 34	62 (-5)	+10
Acidentalmente encontrar material online que promove ódio racial ou extremismo religioso	57	Nada 36/52	45 (+1)	-4
Ciberataques que impedem o seu acesso a serviços online, como banca ou serviços públicos	53	Nada 34/58	59 (+5)	=
Pedirem um pagamento em troca da recuperação do controlo sobre o seu dispositivo	65	Nada 35/44	51 (-6)	=
Receber emails fraudulentos ou telefonemas a pedir os seus dados pessoais (incluindo acesso ao computador, login, informação de pagamentos ou bancária)	61	Nada 32/55	43 (-7)	+9
Fraude online em que os bens adquiridos não são entregues, são contrafeitos ou não são como publicitados	74	Cont. vend. 44/ Cont. vend. 41	74 (-5)	+11

*Esta pergunta é realizada pela primeira vez no inquérito de 2018, Eurobarómetro 480, não permitindo, por isso, realizar comparações com os anos anteriores.

Tabela 12 | Eurobarómetro 499 e 480

Situação com mais reação por cada resposta possível

	Situação com mais reação PT 2019	Valores PT 2019	Situação com mais reação UE 2019	Valores UE 2019
Nada	*Roubo de identidade…*	37	*Receber emails fraudulentos…*	55
Contactaram a polícia	*Ser vítima de fraude em cartão bancário…*	27	*Ser vítima de fraude em cartão bancário…*	31
Contactaram o website/vendedor	*Fraude online em que os bens adquiridos…*	44	*Fraude online em que os bens adquiridos…*	41
Contactaram o fornecedor do serviço de internet	*Roubo de identidade…*	26	*Ocorrer hacking das suas redes…*	16
Contactaram uma organização de proteção do consumidor	*Ocorrer hacking das suas redes…*	7	*Roubo de identidade… ser vítima de fraude em cartão bancário… encontrar pornografia infantil online… fraude online em que os bens adquiridos*	6
Reportaram a situação através de um website ou email oficial (outro que não o da polícia)	*Ser vítima de fraude em cartão bancário… receber emails fraudulentos… ciberataques que impedem o seu acesso… fraude online em que os bens adquiridos…*	6	*Ser vítima de fraude em cartão bancário…*	8
Outro [espontânea]	*Descobrir software malicioso…*	47	*Descobrir software malicioso…*	20
Não sei	*…Encontrar pornografia infantil online…*	15	*Roubo de identidade…*	6

Tabela 13 | Eurobarómetro 499 e 480

Aspetos sociodemográficos relevantes em Portugal, 2019

Sexo | Idade | Educação A variação entre grupos não permite identificar uma tendência. Deve considerar-se o facto de a base estatística ser pouco numerosa como possível fator explicativo (apenas os indivíduos que se reconhecem como vítimas).

UE A tendência mais evidente na média da UE diz respeito à diferença entre sexos, em que as mulheres tendem a reagir um pouco mais do que os homens. A diferença mais relevante refere-se aos ciberataques que impedem o acesso a serviços *online*, como banca ou serviços públicos, em que 64% das mulheres reagiram de algum modo, enquanto apenas 54% dos homens o fizeram.

Eurobarómetro 499

O que fizeram os indivíduos, em Portugal, em cada uma das seguintes situações experienciadas pessoalmente ou de que foram vítimas? (Múltiplas respostas possíveis)
Pelo menos uma ação. 2018-2019. *Vítimas.* (%)

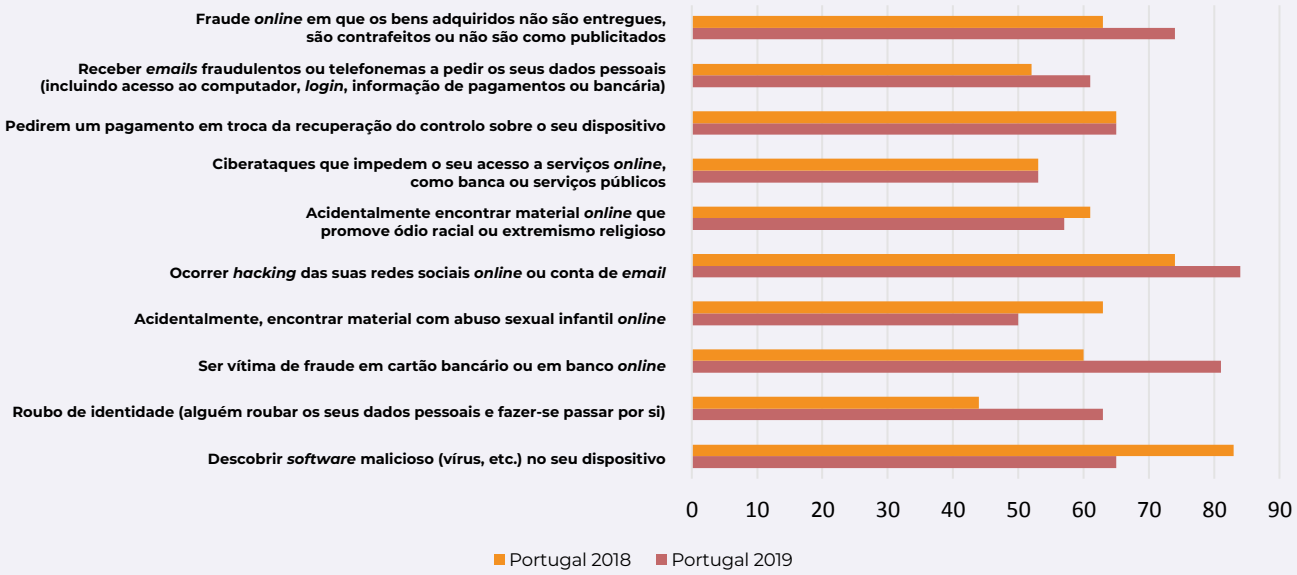


Figura 29 | Eurobarómetro 499 e 480

O que fizeram os indivíduos, em Portugal, em cada uma das seguintes situações experienciadas pessoalmente ou de que foram vítimas? (Múltiplas respostas possíveis) Pelo menos uma ação. Comparação com UE. *Vítimas*. (%)

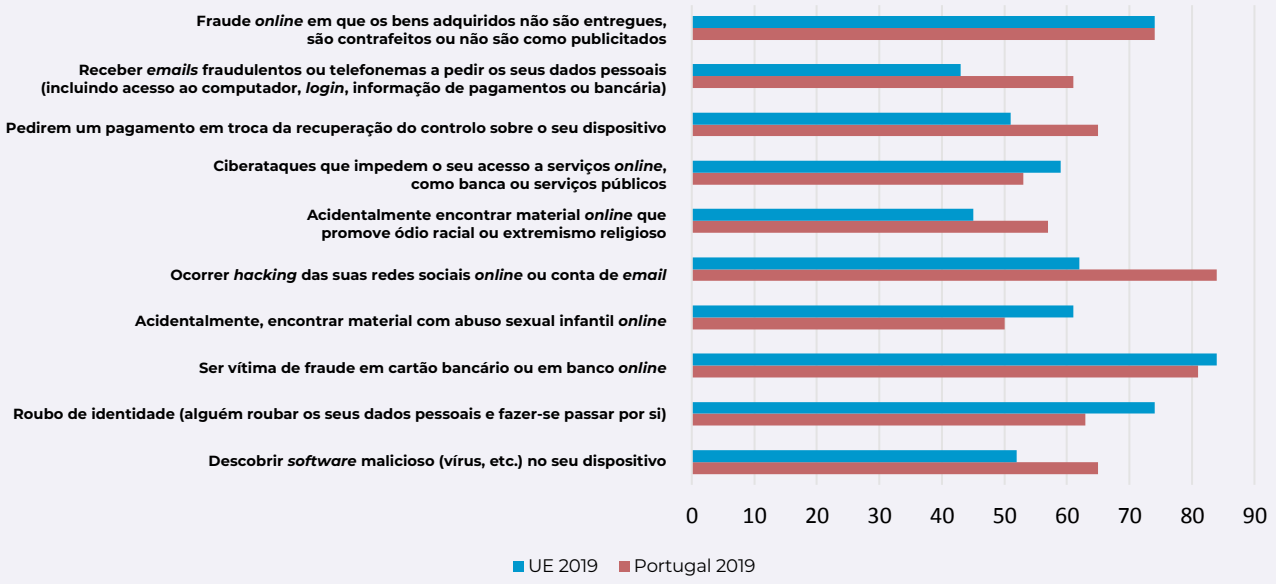


Figura 30 | Eurobarómetro 499

O que fizeram os europeus em cada uma das seguintes situações experienciadas pessoalmente ou de que foram vítimas? (Múltiplas respostas possíveis) Pelo menos uma ação. 2018-2019. *Vítimas*. (%)

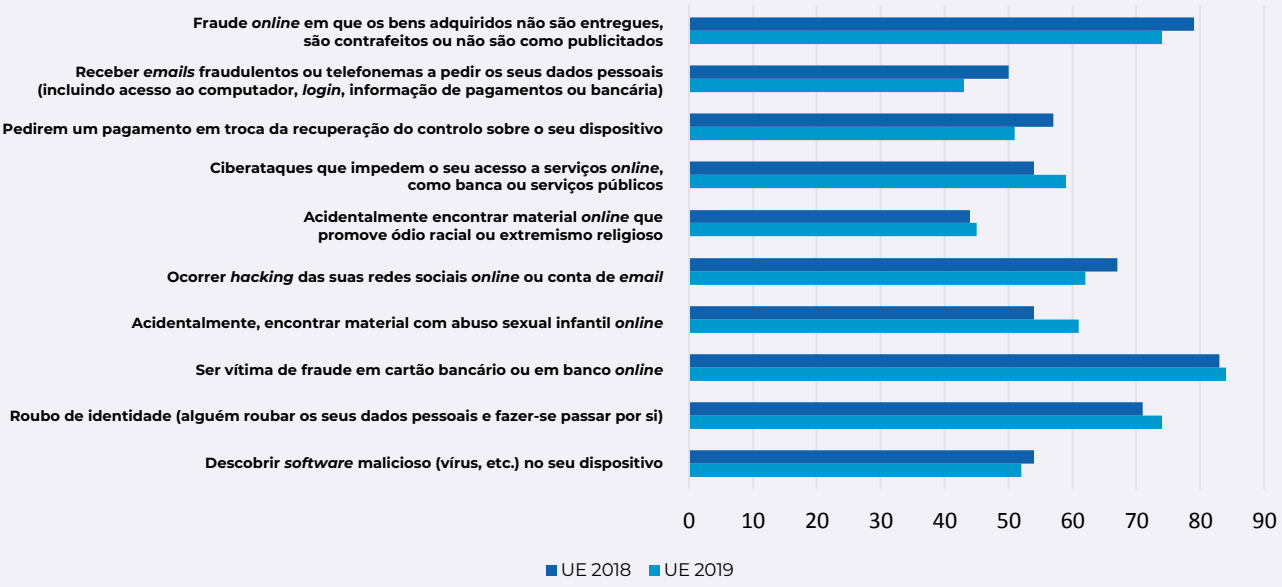


Figura 31 | Eurobarómetro 499 e 480

As situações que mais conduziram a alguma reação por parte das vítimas entre os indivíduos, em Portugal, foram o *hacking* das redes sociais ou conta de *email*, com 84%, e ser vítima de fraude em cartão bancário ou em banco *online*, com 81%. Esta última é a que conduziu a mais reações na média da UE, com 84%. Por sua vez, ocorrer *hacking* das redes sociais *online* ou conta de *email*, na média da UE, apenas atingiu os 62%;

As situações que mais cresceram em termos de reações, entre os indivíduos em Portugal, foram o ser vítima de fraude em cartão bancário ou em banco *online* (+21 pp) e roubo de identidade (+19 pp). As que mais decresceram foram o descobrir *software* malicioso (-18 pp) e, acidentalmente, encontrar pornografia infantil *online* (-13 pp). A média da UE apresentou oscilações menos acentuadas entre 2018 e 2019 (uma explicação possível é o facto de a base da amostra ser muito maior);

Em várias situações, entre os indivíduos em Portugal, a resposta "não se fez nada" teve um volume relevante. Por exemplo, é o caso de 37% das pessoas que foram vítimas de roubo de identidade, enquanto, na mesma situação, 28% na média da UE contactaram a polícia. Comparando com o indicador 7, respeitante àquilo que as pessoas fariam, independentemente de terem sido ou não vítimas, verifica-se um muito menor contacto com a polícia por parte dos indivíduos em Portugal e na média da UE que foram vítimas efetivas destas situações do que entre os que especulam sobre o que fariam caso fossem vítimas;

Existe uma correlação entre o tipo de ação e o tipo de situação: contacta-se mais a polícia quando se é vítima de fraude em cartão bancário ou em banco *online* (27% em Portugal e 31% na média da UE) e o *website*/vendedor quando se é vítima de fraude *online* em que os bens adquiridos não são entregues, são contrafeitos ou não são como publicitados (44% em Portugal e 41% na média da UE).

12. Alguma vez os indivíduos, em Portugal, reportaram um cibercrime ou outro comportamento ilegal *online* (por exemplo, ciberataque, assédio *online* ou *bullying*)? (Múltiplas respostas possíveis). *Todos os indivíduos.* (%)*

	PT 2019	UE 2019
Sim, à polícia ou autoridades	2	7
Sim, a um provedor de serviços	1	5
Sim, a um website	1	6
Sim, a uma organização de proteção do consumidor	1	3
Sim, a outra pessoa	1	3
Não, nunca	95	83
Não sei	1	1
Total "Sim"	4	17

*Questão realizada pela primeira vez em 2019.

Tabela 14 | Eurobarómetro 499

Aspetos sociodemográficos relevantes em Portugal, 2019

Sexo Sem diferenças relevantes entre sexos.

Idade Os indivíduos com mais do que 55 anos de idade tendem a ter reportado menos um cibercrime ou outro comportamento ilegal *online* do que as restantes faixas etárias. Por exemplo, enquanto apenas 1% dos indivíduos com mais do que 55 anos de idade o fizeram, aqueles com idades compreendidas entre os 15 e os 24 anos de idade atingem o valor de 6%.

Educação Os indivíduos que estudaram no máximo até aos 15 anos de idade tendem a reportar menos este tipo de situação do que os restantes grupos, atingindo apenas 2%, enquanto, por exemplo, quem estudou até pelo menos aos 20 anos de idade chega aos 7%.

UE Tendências na média da UE semelhantes aos dados nacionais, exceto no que diz respeito à diferença entre sexos. Na média da UE, os homens apresentam valores ligeiramente superiores quanto a reportar este tipo de situação, com 19%, enquanto as mulheres atingem os 15%.

Eurobarómetro 499

Alguma vez os indivíduos, em Portugal, reportaram um cibercrime ou outro comportamento ilegal *online* (por exemplo, ciberataque, assédio *online* ou *bullying*)? (Múltiplas respostas possíveis) Comparação com UE. *Todos os indivíduos.* (%)

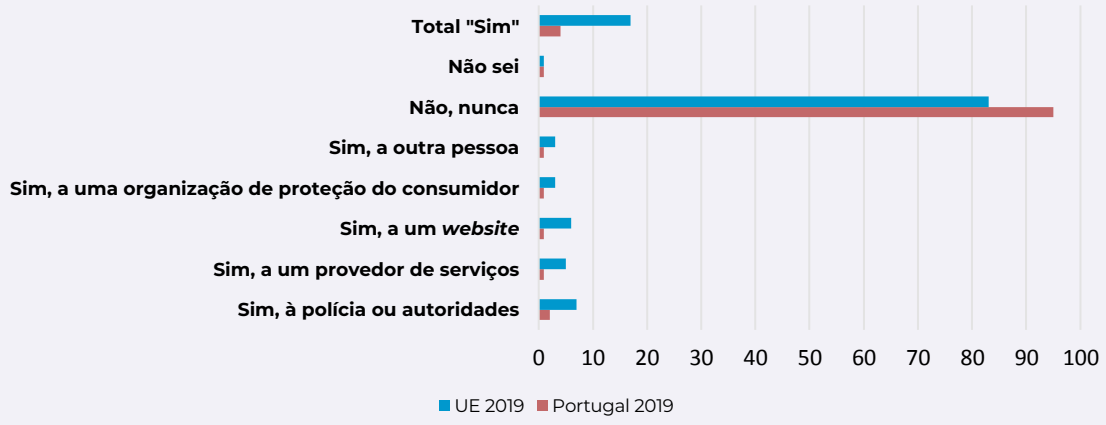


Figura 32 | Eurobarómetro 499

Destaques

Os indivíduos, em Portugal, reportaram menos cibercrimes ou outro comportamento ilegal *online* do que a média da UE, com apenas 4% a afirmarem que já o fizeram alguma vez, enquanto a média da UE atinge os 17%;

Entre os indivíduos, em Portugal, que já reportaram algum cibercrime ou outro comportamento ilegal *online*, a polícia foi o contacto mais frequente já realizado, com 2%, enquanto a média da UE atinge os 7%;

Em Portugal, os indivíduos com menos idade e os indivíduos com mais estudos tendem a ter reportado mais algum cibercrime ou outro comportamento ilegal *online*.

13. Considerando o assédio *online* de crianças com menos de 16 anos (por exemplo, *bullying* ou *grooming*), o que os indivíduos, em Portugal, fazem, se alguma coisa, no seu espaço doméstico, para as proteger enquanto estão *online*? (Múltiplas respostas possíveis) *Todos os indivíduos.* (%)

	PT 2019	UE (tendência 2018-2019)	Tendência PT (2018-2019)	Tendência PT (2017-2018)	Tendência PT* (2014-2017)
O uso da internet pela criança é monitorizado	18	21 (-1)	+5	-1	+3
As configurações de controlo parental são ativadas	5	17 (+3)	-4	-1	=
O tempo gasto pela criança online é limitado	12	19 (=)	-3	=	=
Os riscos online são discutidos com a criança	12	20 (=)	+1	-9	+2
O assédio online é reportado	3	8	**	**	**
Gostaria de fazer algo, mas não sabe como	4	6 (+3)	-2	+3	+2
Outro	7	6 (+2)	+5	=	+1
Nada	11	11 (+6)	+10	-10	+8
Não se aplica	55	52 (=)	-7	+3	-4
Não sabe	9	7 (+5)	+7	+2	-1
Total algo é feito	26	37 (+1)	-3	+1	***

*Questão não realizada em 2013.
** Opção de resposta não disponível nesses anos.
*** Dados indisponíveis.

Tabela 15 | Eurobarómetro 499, 480, 464a e 423

Aspetos sociodemográficos relevantes em Portugal, 2019

Sexo As mulheres tendem a agir mais em relação ao assédio *online* de crianças do que os homens, com 29%, contra 23%, respetivamente.

Idade Os indivíduos com mais de 55 anos de idade tendem a agir menos do que os restantes em relação ao assédio *online* de crianças, com 7% a reconhecerem que agem. Por exemplo, os indivíduos com idades compreendidas entre os 25 e 39 anos atingem os 45%.

Educação Os indivíduos que estudaram no máximo até aos 15 anos de idade tendem a agir menos do que os restantes em relação ao assédio *online* de crianças, com 13%. Os que estudaram até depois dos 20 anos de idade atingem os 45%.

UE Tendências genericamente alinhadas com a média da UE.

Eurobarómetro 499

Considerando o assédio *online* de crianças com menos de 16 anos (por exemplo, *bullying* ou *grooming*), o que os indivíduos, em Portugal, fazem, se alguma coisa, no seu espaço doméstico, para as proteger enquanto estão *online*? (Múltiplas respostas possíveis) 2014-2019. *Todos os indivíduos.* (%)

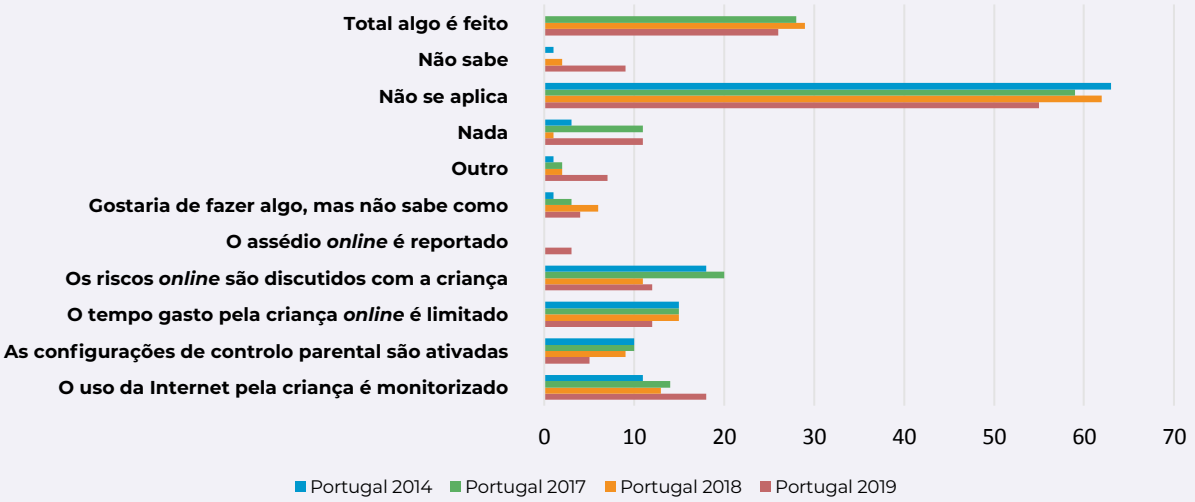


Figura 33 | Eurobarómetro 499, 480, 464a e 423

Considerando o assédio *online* de crianças com menos de 16 anos (por exemplo, *bullying* ou *grooming*), o que os indivíduos, em Portugal, fazem, se alguma coisa, no seu espaço doméstico, para as proteger enquanto estão *online*? (Múltiplas respostas possíveis) *Todos os indivíduos.* (%)

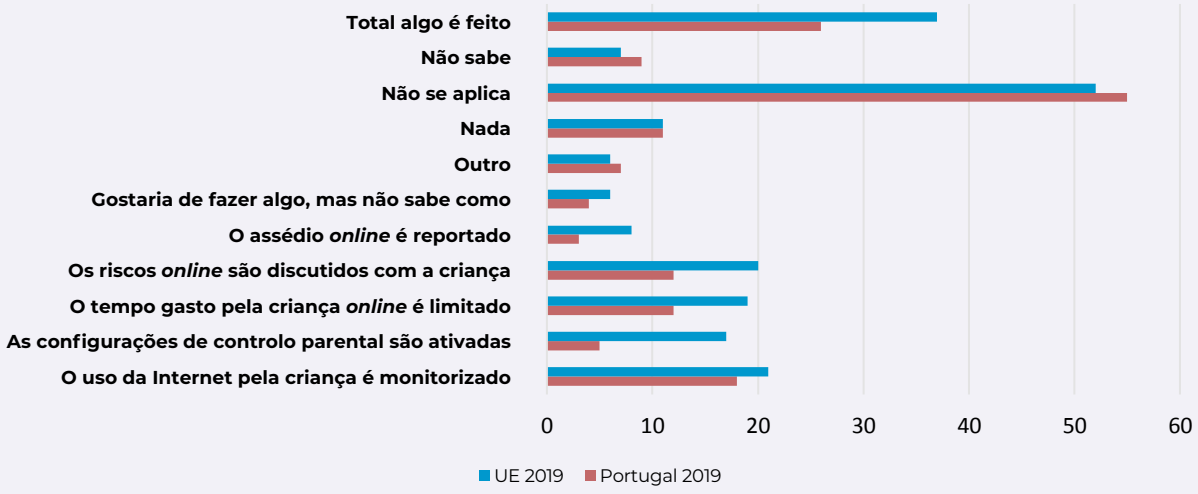


Figura 34 | Eurobarómetro 499 e 480

Considerando o assédio *online* de crianças com menos de 16 anos (por exemplo, *bullying* ou *grooming*), o que os europeus fazem, se alguma coisa, no seu espaço doméstico, para as proteger enquanto estão *online*? (Múltiplas respostas possíveis) 2018-2019. *Todos os indivíduos.* (%)

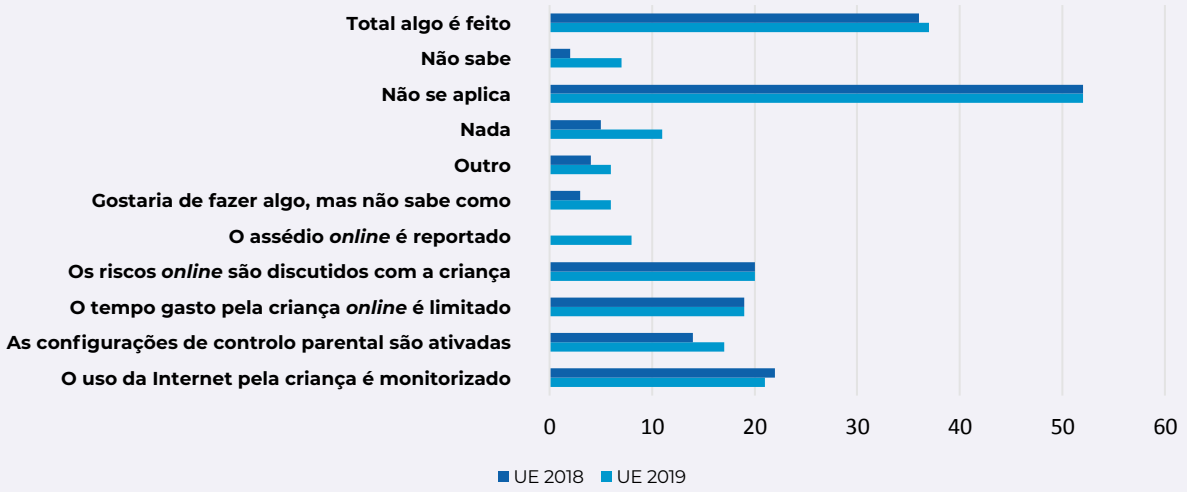


Figura 35 | Eurobarómetro 499 e 480

DESTAQUES

Os indivíduos, em Portugal, tendem a agir menos em relação ao assédio *online* de crianças, com 26% a fazerem algo (menos 3 pp do que em 2018), contra 37% (mais 1 pp do que em 2018) na média da UE;

Aquilo que os indivíduos, em Portugal, mais fazem em relação ao assédio *online* de crianças é a monitorização do uso da Internet pela criança (18%), tal como na média da UE (21%);

Contudo, existem algumas discrepâncias entre os indivíduos em Portugal e a média da UE: apenas 5% ativam as configurações de controlo parental, contra 17% da média da UE; apenas 12% discutem os riscos *online* com os filhos, contra 20% na média da UE; e apenas 12% limitam o tempo gasto pela criança *online*, contra 19% da média da UE;

Em relação ao ano de 2018, houve um aumento de 10 pp de indivíduos, em Portugal, que afirmam que não agiram no que diz respeito ao assédio *online* de crianças.

Durante 2020, o Eurostat atualizou e lançou pela primeira vez um conjunto de indicadores muito relevantes sobre cibersegurança. Um destes indicadores, que não era atualizado desde 2017, é o relativo a *Barreiras Percecionadas Quanto a Comprar/Encomendar Através da Internet* devido a preocupações com a segurança de pagamento (Eurostat, 2020a). O ato de não comprar *online* devido a preocupações de segurança de pagamento é um comportamento que resulta de uma preocupação com a cibersegurança, o que pode ser perspetivado mais como um cuidado do que como um problema, embora o que se pretenda em termos de ciber-higiene seja a realização de compras *online* com cuidado e não o deixar de as fazer.

14. Barreiras percecionadas pelos indivíduos, em Portugal, quanto a comprar/encomendar através da Internet: Preocupações com a segurança de pagamento. (%)

	PT 2019	UE (tendência 2017-2019)	Tendência PT (2017-2019)	Tendência PT (2015-2017)	Tendência PT (2009-2015)
Indivíduos que, nos últimos 12 meses, não compraram/encomendaram bens ou serviços pela Internet para uso privado, devido a preocupações com a segurança de pagamento	23	6 (-1)	-6	+3	+5

Tabela 16 | Eurostat 2020a

Aspetos sociodemográficos relevantes em Portugal, 2019[3]

Sexo As mulheres, com idades compreendidas entre os 16 e os 74 anos, tendem a não comprar/encomendar bens ou serviços pela Internet para uso privado, devido a preocupações com a segurança de pagamento, em maior percentagem, com 24%, do que os homens, com 21%, na mesma faixa etária.

Idade Os indivíduos com idades compreendidas entre os 25 e os 34 anos tendem a restringir menos a sua ação a este respeito, com 14%, do que as restantes faixas etárias. Por exemplo, quem tem idades compreendidas entre os 45 e os 54 anos de idade apresenta o valor de 28%.

Educação Os indivíduos com uma educação formal superior e idades entre os 25 e os 64 anos também tendem a restringir menos a sua ação, com 18%. Quem tem uma educação formal baixa e média restringe mais, com 27% cada, na mesma faixa etária.

UE Na média da UE verifica-se mais equilíbrio entre sexos. Contudo, nos restantes domínios a tendência é semelhante aos dados sobre Portugal.

Eurostat 2020a

3 Nos dados do Eurostat, os grupos etários correspondem aos seguintes intervalos: até 15 anos; 16-24 anos; 25-34 anos; 35-54 anos; 55-64 anos; 65-74 anos; +75 anos. Os grupos educacionais, aos seguintes tipos: educação formal baixa, média ou superior.

Indivíduos, em Portugal, nos últimos 12 meses, não compraram/encomendaram bens ou serviços pela Internet para uso privado, devido a preocupações com a segurança de pagamento. 2009-2019. *Todos os indivíduos.* (%)

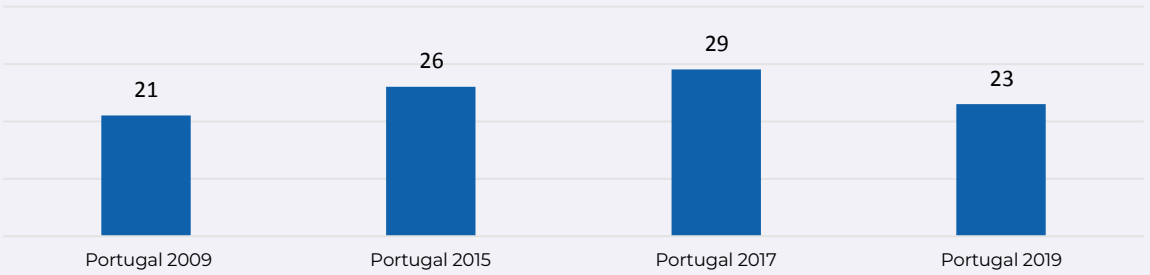


Figura 36 | Eurostat 2020a

Indivíduos, em Portugal, nos últimos 12 meses, não compraram/encomendaram bens ou serviços pela Internet para uso privado, devido a preocupações com a segurança de pagamento. Comparação com a UE. *Todos os indivíduos.* (%)

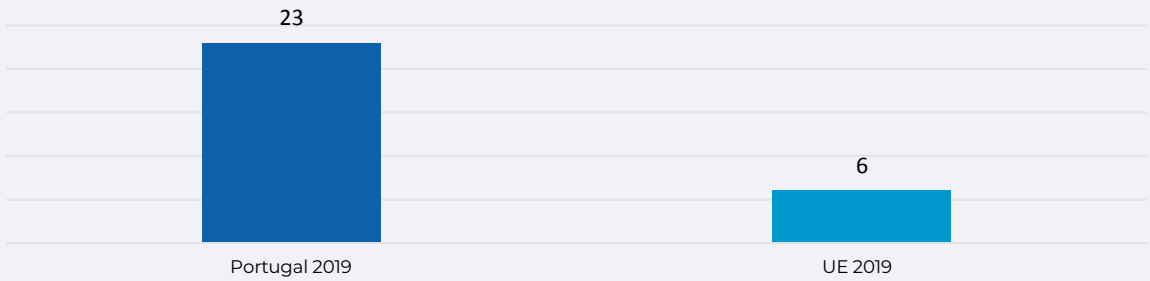


Figura 37 | Eurostat 2020a

Europeus que, nos últimos 12 meses, não compraram/encomendaram bens ou serviços pela Internet para uso privado, devido a preocupações com a segurança de pagamento. 2017-2019. *Todos os indivíduos.* (%)

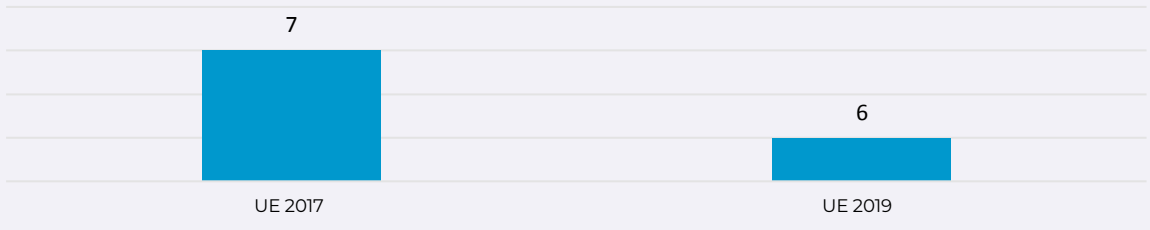


Figura 38 | Eurostat 2020a

Destaques

Os indivíduos, em Portugal, não compraram/encomendaram bens ou serviços pela Internet para uso privado, devido a preocupações com a segurança de pagamento, em percentagem superior à média da UE, atingindo os 23%, enquanto a média da UE atinge apenas os 6%;

Não obstante, a tendência é decrescente em relação ao ano de 2017, entre os indivíduos, em Portugal, com menos 6 pp, depois de subidas contínuas nos inquéritos anteriores;

Em Portugal, os homens, os que têm idades compreendidas entre os 24 e os 35 anos e os que têm uma educação superior restringem menos a sua ação de comprar/encomendar bens ou serviços pela Internet para uso privado, devido a preocupações com a segurança de pagamento, do que os restantes grupos.

Também do Eurostat (2020b), o indicador sobre *Cópias de Segurança e Ficheiros de Backup* diz respeito a um comportamento de cuidado por parte dos indivíduos que é relevante considerar. Trata-se de uma ação que promove, por exemplo, uma melhor proteção contra o *ransomware*, o qual, cifrando os dados da vítima e pedindo um resgate para os decifrar, pode ser contornado com um *backup*, de preferência desconectado da Internet. Este indicador refere-se exclusivamente a 2019.

15. Cópias de segurança e ficheiros de *backup*, em Portugal, 2019. *Todos os indivíduos.* (%)*

	PT	UE
Portugueses que fazem cópias de segurança dos seus ficheiros num dispositivo externo de armazenamento ou num espaço de armazenamento na Internet, automática ou manualmente	39	48

*Esta questão tem um formato diferente nos anos anteriores.
Por isso, apenas se apresentam dados relativos a 2019.

Tabela 17 | Eurostat 2020b

Aspetos sociodemográficos relevantes Portugal 2019

Sexo Os homens, entre os 16 e os 74 anos de idade, tendem mais do que as mulheres com as mesmas idades a fazer cópias de segurança dos seus ficheiros nas condições descritas, em 41%, enquanto as mulheres atingem os 37%.

Idade Os indivíduos mais novos tendem a fazer mais cópias deste tipo do que os mais velhos. Por exemplo, os indivíduos com idades compreendidas entre os 16 e os 24 anos apresentam o registo de 62%, enquanto os que têm entre 65 e 74 anos atingem apenas os 11%.

Educação Os indivíduos com educação formal superior e idades compreendidas entre os 25 e os 64 anos fazem mais cópias de segurança dos seus ficheiros, com 77%, do que os que têm educação formal média, com 51%, e baixa, com 15%, na mesma faixa etária.

UE Tendências alinhadas com a média da UE.

Eurostat 2020b

Indivíduos, em Portugal, que fazem cópias de segurança dos seus ficheiros num dispositivo externo de armazenamento ou num espaço de armazenamento na Internet, automatica ou manualmente. *Todos os indivíduos.* (%)

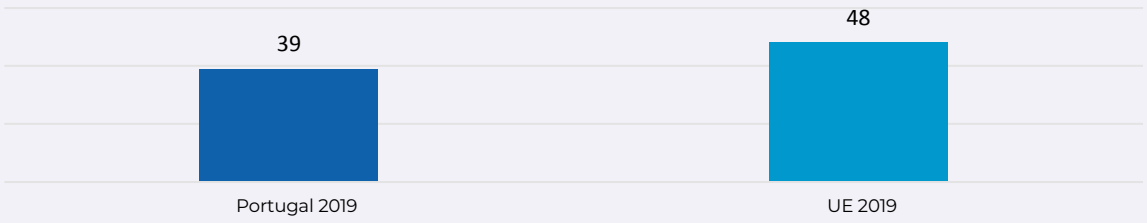


Figura 39 | Eurostat 2020b

Destaques

Os indivíduos, em Portugal, fazem menos cópias de segurança dos seus ficheiros num dispositivo externo de armazenamento ou num espaço de armazenamento na Internet, automática ou manualmente, do que a média da UE, com 39%, contra 48%, respetivamente;

Em Portugal, os homens, os indivíduos mais novos e os que têm uma educação formal superior tendem a fazer mais cópias de segurança do tipo descrito do que os restantes grupos.

COMPORTAMENTOS ORGANIZACIONAIS

EMPRESAS

Este ano é possível ter acesso a um conjunto de indicadores sobre empresas muito relevante, fruto do lançamento, durante 2020, dos resultados do inquérito do Eurostat sobre *Políticas de Segurança: medidas, riscos e sensibilização de colaboradores* (Eurostat, 2020c). Através desta fonte, apresentam-se números sobre medidas de cibersegurança que as empresas aplicam, a sua definição de políticas a este respeito, a existência ou não de recomendações documentadas e ainda o modo como se organizam as atividades relacionadas com a segurança das TIC. A componente deste inquérito ligada à sensibilização é remetida para o capítulo sobre Educação e Sensibilização.

16. Medidas de segurança das TIC nas empresas[4], em Portugal, 2019. (%)

	Todas		Pequenas		Médias		Grandes	
	PT	UE	PT	UE	PT	UE	PT	UE
Autenticação forte de password	85	77	83	75	91	86	96	93
Manter o software (incluindo sistemas operativos) atualizado	90	87	89	86	95	94	97	97
Identificação do utilizador e autenticação através de métodos biométricos implementados pela empresa	15	10	12	8	*	14	38	22
Técnicas de cifra para dados, documentos ou emails	39	38	37	34	*	53	73	72
Backup de dados para um local separado (incluindo backup para a nuvem)	74	76	71	74	89	86	93	91
Controlo de acesso à rede (gestão do acesso de dispositivos e utilizadores à rede da empresa)	71	64	67	60	90	81	96	89
VPN (uma Rede Virtual Privada cria uma rede privada através de uma rede pública para permitir a troca segura de dados nessa rede pública)	42	42	36	36	*	67	91	87
Guardar logs para análise depois de incidentes de segurança	58	45	55	40	*	66	85	82
Avaliação de risco de TIC, i. e., avaliação periódica das probabilidades e consequências de incidentes de segurança de TIC	41	34	37	29	*	54	76	72
Testes de segurança das TIC	43	36	38	31	*	55	78	74
Empresas a usar alguma medida de segurança das TIC	98	93	97	92	100	97	100	99

* Dados indisponíveis.

Tabela 18 | Eurostat 2020c

4 No âmbito do Eurostat, todas as empresas: 10 trabalhadores ou mais; pequenas: 10-49 trabalhadores; médias: 50-249 trabalhadores; grandes: 250 ou mais trabalhadores. As sociedades financeiras não estão incluídas.

Medidas de segurança das TIC nas empresas, em Portugal. Comparação com UE.
Todas as empresas. (%)

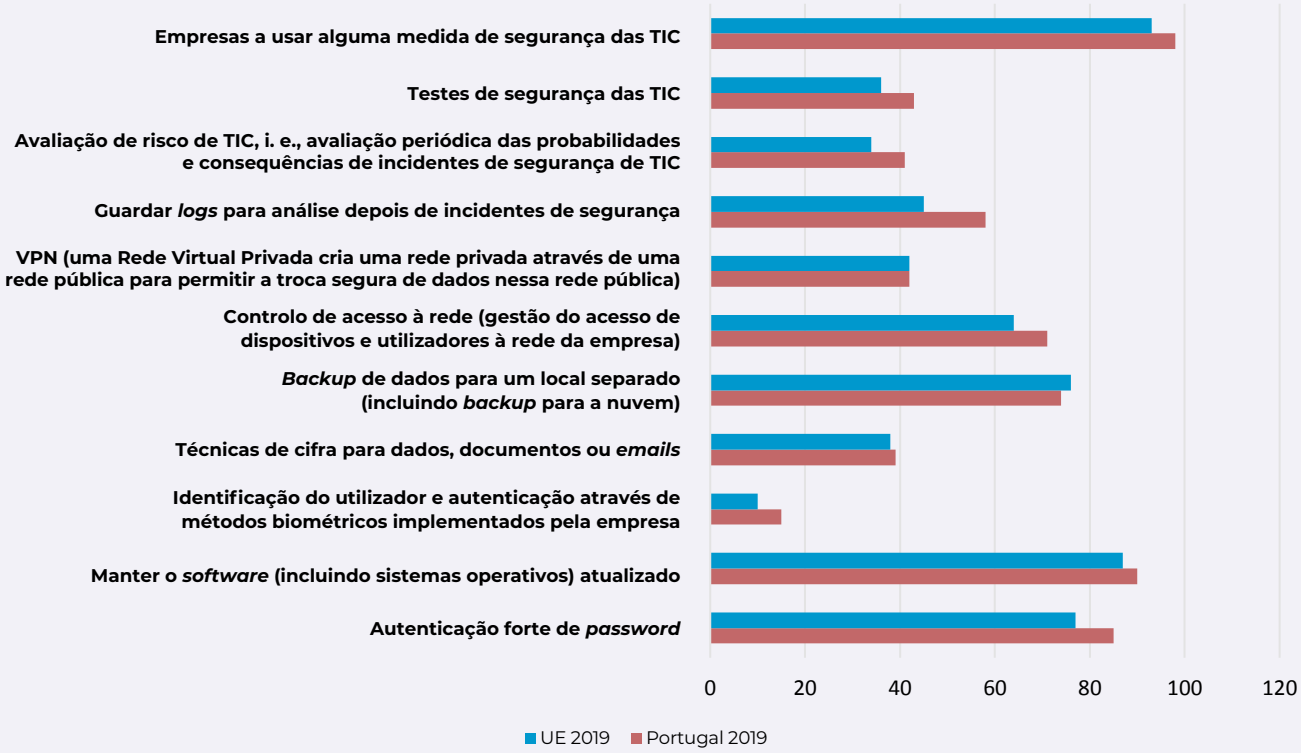


Figura 40 | Eurostat 2020c

Destaques

As empresas, em Portugal, aplicam mais medidas de segurança, com 98%, do que a média da UE, com 93%, considerando todas as empresas;

A medida mais aplicada entre todas as empresas, em Portugal, é a manutenção do *software* atualizado, com 90%. Também é a medida mais comum na média da UE, com 87%;

A medida menos frequente entre todas as empresas, em Portugal, é a identificação do utilizador e autenticação através de métodos biométricos, com 15%. A média da UE atinge os 10%;

As grandes empresas, em Portugal, aplicam mais medidas do que as pequenas, com 100% e 97%, respetivamente, que aplicam pelo menos uma medida, tendência que também se verifica na média da UE.

17. Políticas de segurança das TIC nas empresas, em Portugal. (%)

	Todas 2019		Tendência 2015-2019		Pequenas 2019		Médias 2019		Grandes 2019	
	PT	UE	PT	UE	PT	UE	PT	UE	PT	UE
A política de segurança das TIC da empresa foi definida ou revista pela última vez nos últimos 12 meses	21	26	-8	+6	18	23	*	41	59	60
A política de segurança das TIC da empresa foi definida ou revista pela última vez há mais de 12 meses, até há 24 meses	5	6	-3	=	4	5	8	10	11	12
A política de segurança das TIC da empresa foi definida ou revista pela última vez há mais de 24 meses	2	2	-9	-3	2	2	4	3	4	4
Total com política de segurança das TIC	28	34	-20	+3	24	30	12	54	74	76

* Dados indisponíveis.

Tabela 19 | Eurostat 2020c

Política de segurança das TIC nas empresas, em Portugal. 2015-2019. *Todas as empresas.* (%)

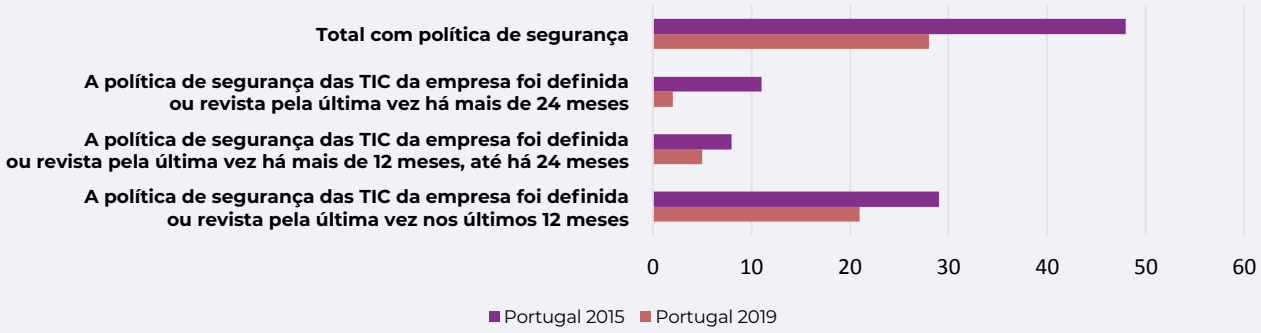


Figura 41 | Eurostat 2020c

Política de segurança das TIC nas empresas, em Portugal. Comparação com UE. *Todas as empresas.* (%)

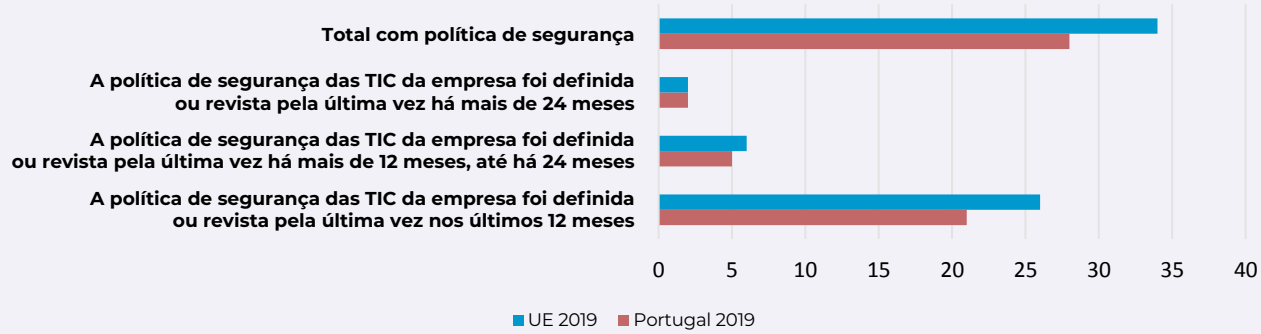


Figura 42 | Eurostat 2020c

Política de segurança das TIC nas empresas europeias. 2015-2019. *Todas as empresas*. (%)

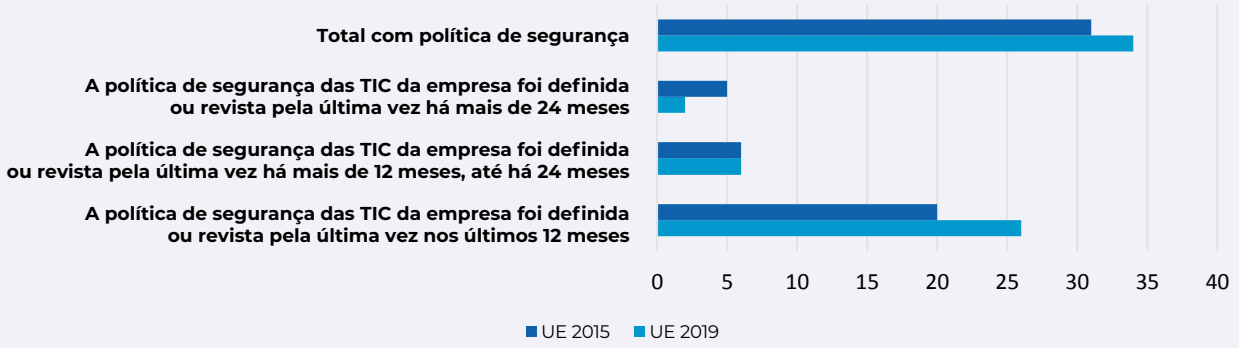


Figura 43 | Eurostat 2020c

DESTAQUES

Existem menos empresas, em Portugal, com políticas de segurança das TIC definidas ou revistas, com 28%, do que a média da UE, que atinge os 34%, independentemente de há quanto tempo têm essa política definida;

Entre todas as empresas, em Portugal, que possuem uma política de segurança das TIC, a maioria definiu ou reviu essa política nos últimos 12 meses à realização do inquérito;

Existe uma maior percentagem de grandes empresas do que entre os restantes tipos de empresas a ter uma política de segurança das TIC, com 74% em Portugal e 76% na média da UE.

18. Empresas, em Portugal, que possuem recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC e assuntos considerados, 2019. (%)

	Todas		Pequenas		Médias		Grandes	
	PT	UE	PT	UE	PT	UE	PT	UE
Empresas que possuem recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC	28	34	24	30	*	54	74	76
Assuntos considerados nessas recomendações: gestão dos níveis de acesso ao uso das TIC	26	30	22	25	*	49	71	71
Assuntos considerados nessas recomendações: armazenamento, proteção, acesso e processamento de dados	27	31	23	26	*	49	73	71
Assuntos considerados nessas recomendações: procedimentos ou regras para prevenir ou responder a incidentes de segurança	24	24	20	20	*	41	65	63
Assuntos considerados nessas recomendações: responsabilidades, direitos e deveres no que diz respeito à utilização das TIC	26	28	22	23	*	46	71	68
Assuntos considerados nessas recomendações: formação do pessoal ao serviço para uma utilização segura das TIC	21	22	17	18	*	37	60	58

* Dados indisponíveis.

Tabela 20 | Eurostat 2020c

Empresas, em Portugal, que possuem recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC e assuntos considerados. Comparação com UE. *Todas as empresas*. (%)

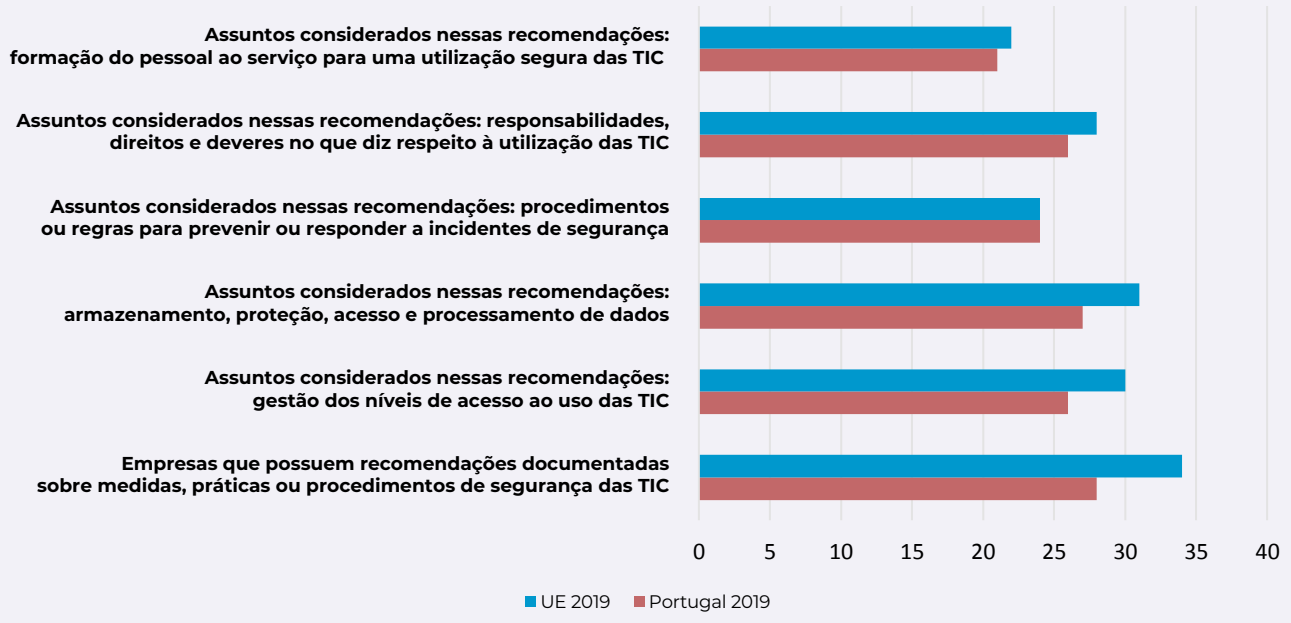


Figura 44 | Eurostat 2020c

Existem menos empresas, em Portugal, do que a média da UE a terem recomendações documentadas sobre medidas, práticas e procedimentos em segurança das TIC, com 28% e 34%, respetivamente;

O tipo de assunto mais considerado nestas recomendações, quer em Portugal, quer na média da UE, é o armazenamento, proteção, acesso e processamento de dados, com 27% e 31%, respetivamente;

As grandes empresas são as que apresentam percentagens maiores a todos os níveis no que diz respeito a ter recomendações documentadas e aos assuntos que estas incluem. Por exemplo, 74% das grandes empresas, em Portugal, possuem este tipo de recomendação documentada. A média da UE é de 76%. Apenas 24% das pequenas empresas, em Portugal, e 30% na média da UE têm recomendações documentadas deste tipo.

19. Realização das atividades relacionadas com a segurança das TIC nas empresas, em Portugal, 2019. (%)

	Todas		Pequenas		Médias		Grandes	
	PT	UE	PT	UE	PT	UE	PT	UE
As atividades relacionadas com a segurança das TIC são realizadas pelos colaboradores da empresa	46	41	43	37	*	58	89	83
As atividades relacionadas com a segurança das TIC são realizadas por fornecedores externos	75	63	75	62	*	68	68	67
As atividades relacionadas com a segurança das TIC são realizadas pelos colaboradores da empresa ou por fornecedores externos	98	85	98	83	100	94	100	98

* Dados indisponíveis.

Tabela 21 | Eurostat 2020c

Realização das atividades relacionadas com a segurança das TIC nas empresas, em Portugal, 2019. Comparação com UE. *Todas as empresas*. (%)

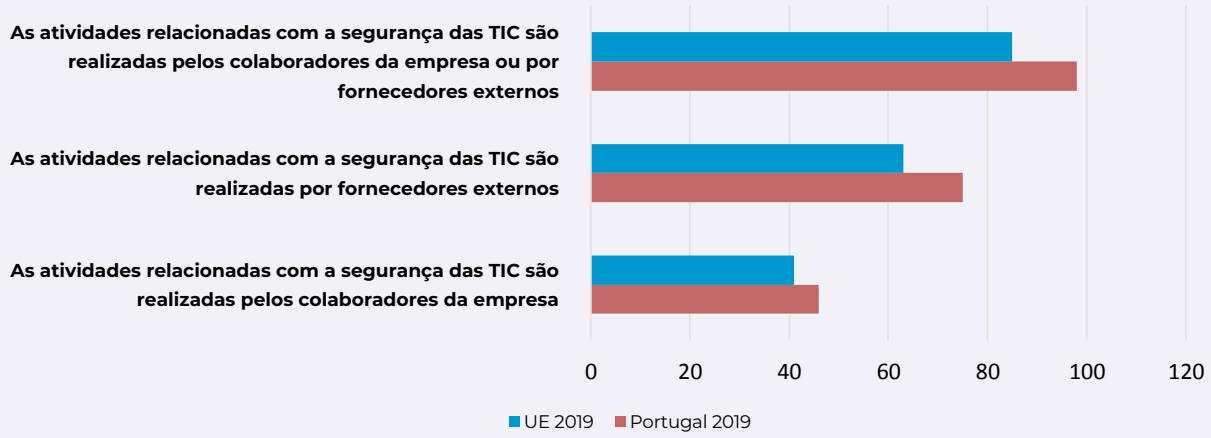


Figura 45 | Eurostat 2020c

DESTAQUES

As empresas, em Portugal, recorrem mais a fornecedores externos, em 75% das atividades relacionadas com a segurança das TIC, do que a colaboradores da empresa, em 46% das atividades (algumas atividades são realizadas pelos dois tipos de recursos). Esta tendência também se verifica na média da UE, com 63% e 41%, respetivamente.

ADMINISTRAÇÃO PÚBLICA CENTRAL E REGIONAL E CÂMARAS MUNICIPAIS

Continuando com um pendor organizacional, mas desta feita orientado ao setor público, os indicadores do IUTIC para a Administração Pública Central e Regional (IUTICAP) e para as Câmaras Municipais (IUTICCM), da DGEEC, respeitantes a 2019 e publicados em 2020, são muito importantes (DGEEC, 2020a e 2020b). Estes dados, que incidem sobre todo o universo, em lugar de resultarem de uma amostra, têm uma fiabilidade muito grande. Em muitos aspetos, reproduzem o inquérito do Eurostat sobre Políticas de Segurança (aplicado pelo INE) (Eurostat, 2020c), mas neste outro contexto e sem comparação com a média da UE. É possível encontrar nesta fonte indicadores sobre a definição de políticas de segurança, recursos humanos na área da cibersegurança, medidas de segurança das TIC adotadas e recomendações documentadas.

20. Entidades da Administração Pública que têm definida uma estratégia para a segurança de informação, em Portugal. *Administração Pública Central e Regional e Câmaras municipais.* (%)

	2019	Tendência PT (2018-2019)	Tendência PT (2017-2018)
Administração Pública Central	68	-4	+5
Administração Pública Regional dos Açores	55	+3	+7
Administração Pública Regional da Madeira	33	+7	-4
Câmaras Municipais	67	+2	+6

Tabela 22 | DGEEC 2020a e 2020b

Entidades da Administração Pública que têm definida uma estratégia para a segurança de informação, em Portugal. 2017-2019. *Administração Pública Central e Regional e Câmaras Municipais.* (%)

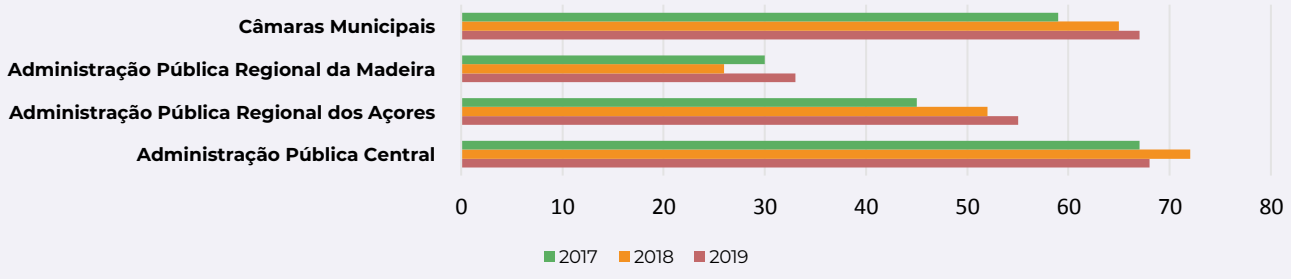


Figura 46 | DGEEC 2020a e 2020b

Destaques

Os organismos da Administração Pública Central e as Câmaras Municipais são as entidades públicas que mais indicaram ter uma estratégia para a segurança de informação definida, com 68% e 67%, respetivamente. No caso da Administração Pública Central os valores representam uma diminuição em relação ao ano anterior em 4 pp, e, nas Câmaras Municipais, um crescimento de 2 pp;

Verifica-se um crescimento deste indicador em 7 pp em relação a 2018 entre os organismos da Administração Pública Regional da Madeira, para 33% (ainda assim, o valor mais baixo).

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

	2019	Tendência PT (2018-2019)	Tendência PT (2017-2018)
Administração Pública Central	34	=	+1
Administração Pública Regional dos Açores	28	+8	-5
Administração Pública Regional da Madeira	29	-4	+10
Câmaras Municipais	45	+8	-1

Tabela 23 | DGEEC 2020a e 2020b

Entidades da Administração Pública, em Portugal, que indicaram ter elevada necessidade de reforço de competências em segurança das TIC. 2017-2019. *Administração Pública Central e Regional e Câmaras Municipais. (%)*

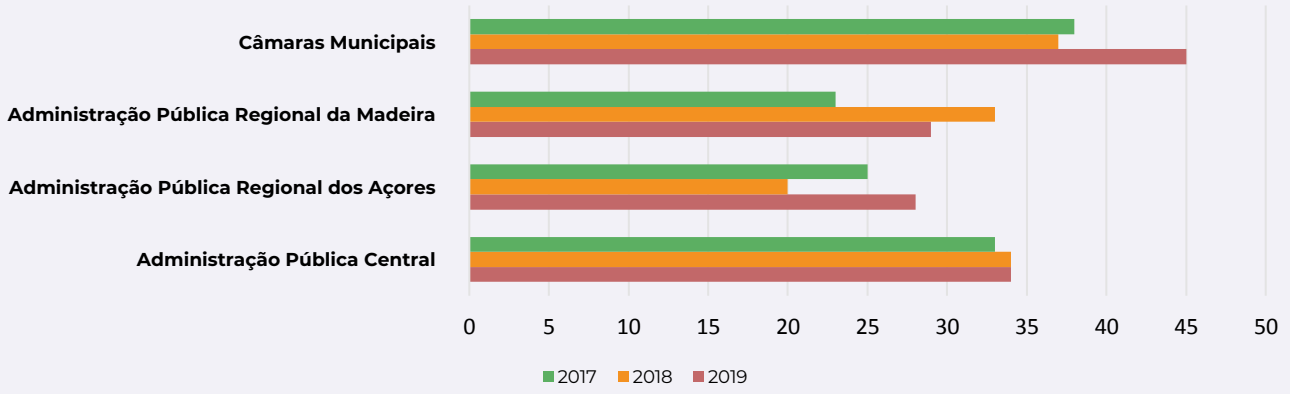


Figura 47 | DGEEC 2020a e 2020b

DESTAQUES

As Câmaras Municipais, com 45%, são o tipo de entidade que mais refere ter elevada necessidade de reforçar competências em matéria de segurança das TIC, representando mais 8 pp do que o ano de 2018.

22. Medidas de segurança das TIC utilizadas em entidades públicas, em Portugal, 2019. ***Administração Pública Central e Regional e Câmaras Municipais.*** **(%)**

	AP Central	AP Açores	AP Madeira	CM
Atualização regular do software	95	100	89	100
Controlo de acessos à rede do Organismo	89	98	89	93
Autenticação dos utilizadores através de uma palavra-passe segura	88	91	82	85
Conservação de registos para análise depois da ocorrência de incidentes de segurança	79	75	58	68
Avaliação dos riscos ligados às TIC	59	43	47	50
Testes da segurança às TIC	56	62	42	49
Técnicas de encriptação de dados, documentos ou emails	55	47	42	47
Identificação e autenticação do utilizador através de métodos biométricos	27	43	33	42

Tabela 24 | DGEEC 2020a e 2020b

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

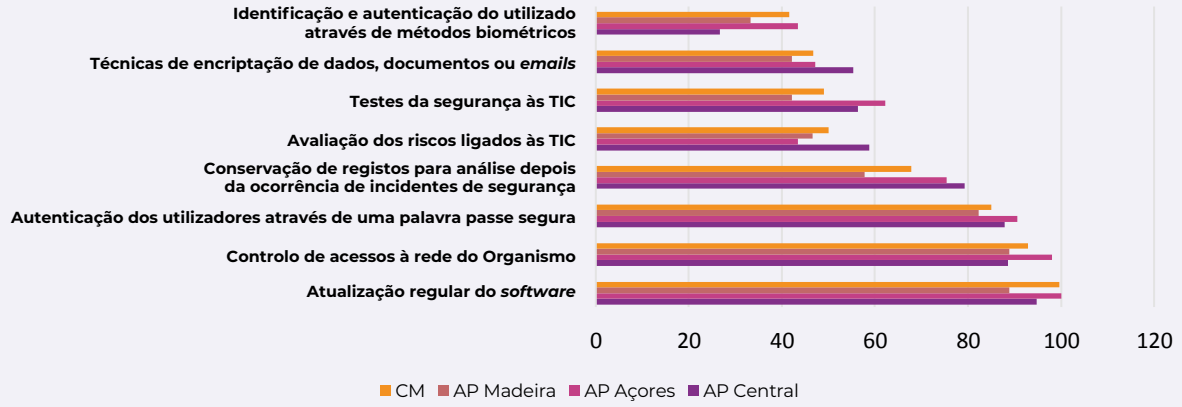


Figura 48 | DGEEC 2020a e 2020b

DESTAQUES

O tipo de medida de segurança das TIC mais implementada, entre as entidades da Administração Pública Central e Regional e Câmaras Municipais, em Portugal, em 2019, é a atualização regular do *software*, com valores entre os 89% (AP Madeira) e os 100% (AP Açores e CM);

O tipo de medida menos utilizada é a identificação e autenticação do utilizador através de métodos biométricos, com valores entre os 27% (AP Central) e os 43% (AP Açores).

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

	AP Central	AP Açores	AP Madeira	CM
Pessoal do próprio Organismo (apenas)	43	58	62	44
Fornecedores externos (apenas)	18	21	29	8
Pessoal do próprio Organismo e fornecedores externos	39	21	9	47

Tabela 25 | DGEEC 2020a e 2020b

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

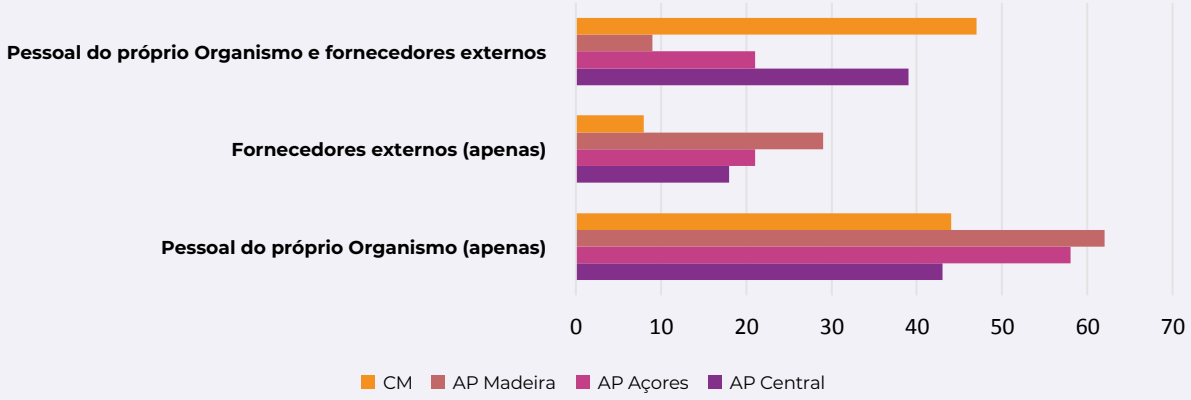


Figura 49 | DGEEC 2020a e 2020b

DESTAQUES

O pessoal do próprio Organismo é, na sua maioria, quem realiza as atividades relacionadas com a segurança das TIC, entre as entidades da Administração Pública Central e Regional e Câmaras Municipais, com valores entre os 43% (AP Central) e os 63% (AP Madeira). Contudo, nas Câmaras Municipais, a maioria das atividades deste tipo são realizadas por uma combinação de pessoal do próprio Organismo e fornecedores externos, em 47% das entidades.

24. Entidades da Administração Pública que possuem recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC e assuntos considerados nas mesmas, em Portugal, 2019. *Administração Pública Central e Regional e Câmaras Municipais.* (%)

	AP Central	AP Açores	AP Madeira	CM
Organismos que possuem recomendações documentas sobre medidas, práticas ou procedimentos de segurança das TIC	52	36	29	36
Assuntos considerados nessas recomendações: gestão dos níveis de acesso às TIC	93	95	92	92
Assuntos considerados nessas recomendações: armazenamento, proteção, acesso e processamento de dados	93	95	92	88
Assuntos considerados nessas recomendações: responsabilidade, direitos e deveres no que respeita à utilização das TIC	92	89	77	89
Assuntos considerados nessas recomendações: procedimentos ou regras para prevenir ou reagir a incidentes de segurança	77	68	92	75
Assuntos considerados nessas recomendações: formação do pessoal ao serviço para uma utilização segura das TIC	68	68	77	56

Tabela 26 | DGEEC 2020a e 2020b

Entidades da Administração Pública que possuem recomendações documentadas sobre medidas práticas ou procedimentos de segurança das TIC e assuntos considerados nas mesmas, em Portugal, 2019. *Administração Pública Central e Regional e Câmaras Municipais.* (%)

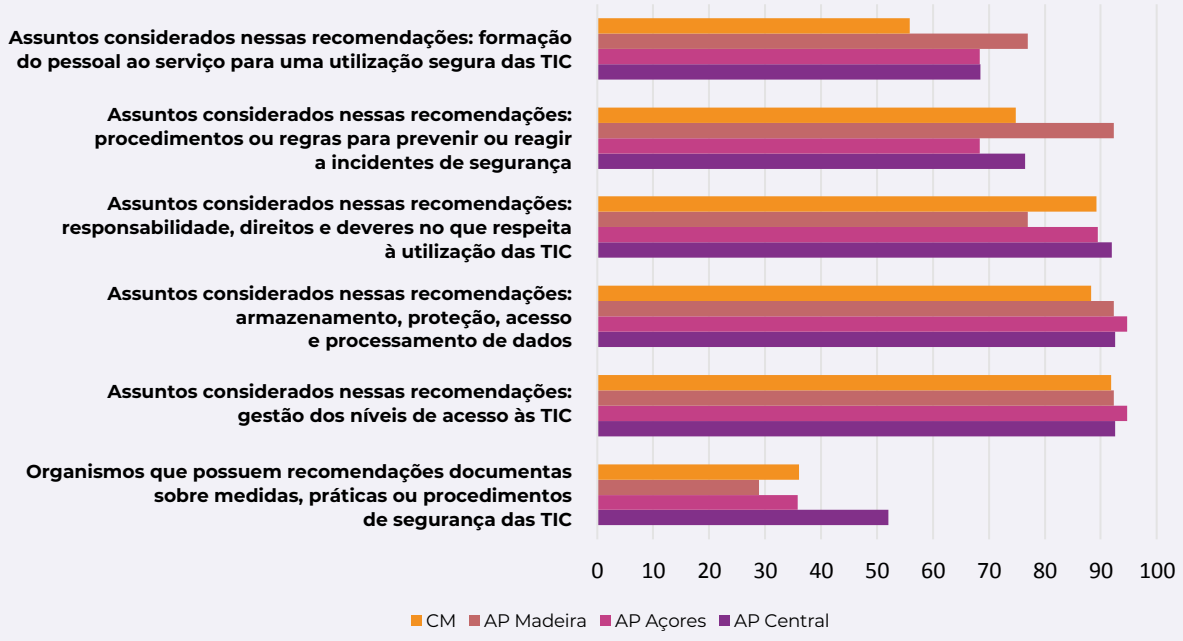


Figura 50 | DGEEC 2020a e 2020b

A Administração Pública Central é a que tem mais entidades com recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC, com 52%;

As entidades da Administração Pública Regional da Madeira são as que possuem menos destas recomendações, com 29% - não obstante, este tipo de Organismo apresenta um valor elevado quanto ao assunto considerado nessas recomendações relativo a procedimentos ou regras para prevenir ou reagir a incidentes de segurança, com 92%, enquanto as restantes entidades apresentam valores entre os 68% (AP Açores) e os 77% (AP Central);

Os tipos de assuntos mais frequentes nestes documentos são: gestão de níveis de acesso (entre os 92% e os 95%) e o armazenamento, proteção, acesso e processamento de dados (entre os 88% e os 95%);

O assunto menos frequente incluído nesta documentação é a formação do pessoal ao serviço para uma utilização segura das TIC, com valores entre os 56% (CM) e os 77% (AP Madeira).

Síntese – Os Comportamentos Individuais, em Portugal, face à Cibersegurança

O cuidado em não abrir *emails* de pessoas desconhecidas é a ação mais frequente, entre os indivíduos, utilizadores de Internet, em resultado de preocupações com a Internet. Em geral, há uma ligeira subida no que diz respeito às mudanças de comportamento neste âmbito.

O tipo de cuidado que mais subiu em 2019 em relação ao ano de 2018 foi a utilização de *passwords* diferentes em *websites* diversos e o que mais decresceu foi a instalação de um antivírus.

Os indivíduos, utilizadores de Internet, mudam menos as suas *passwords* do que a média da UE. O *email* é o tipo de conta em que esta mudança mais ocorre.

Os indivíduos, utilizadores de Internet, reconhecem menos do que a média da UE ter sido vítimas de cibercrimes.

As ciberameaças que mais conduziram as vítimas a uma reação foi o *hacking* das suas redes sociais *online* ou conta de *email*.

Ao contrário dos indivíduos que afirmam que contactariam a polícia caso fossem vítimas de certas ciberameaças, na realidade, aqueles que foram efetivamente vítimas, na sua maioria, realizaram outras ações ou não fizeram nada.

Os indivíduos fazem menos reporte de cibercrimes do que a média da UE.

Os indivíduos agem menos do que a média da UE em relação ao assédio *online* de crianças (em decrescimento em relação a 2018). Quando agem, o que fazem mais é monitorizar a criança.

A discussão sobre os riscos *online* com os filhos continua, tal como em 2018, abaixo da média da UE.

Há mais indivíduos do que a média da UE a não comprar/encomendar bens ou serviços pela Internet para uso privado, devido a preocupações com a segurança de pagamento.

Os indivíduos fazem menos cópias de segurança do que a média da UE.

Síntese – Os Comportamentos Organizacionais, em Portugal, face à Cibersegurança

As empresas afirmam aplicar medidas de segurança das TIC em maior percentagem do que a média da UE.

Há menos empresas do que a média da UE com políticas de segurança das TIC definidas ou revistas.

Também existem menos empresas do que a média da UE com recomendações documentadas sobre medidas, práticas e procedimentos em segurança das TIC.

Enquanto as empresas recorrem mais a fornecedores externos, as entidades públicas consideradas recorrem mais a colaboradores internos para atividades relacionadas com a segurança das TIC.

A maioria das entidades da Administração Pública Central e Regional e Câmaras Municipais tem uma estratégia de segurança da informação definida.

As Câmaras Municipais, entre as entidades públicas, são o tipo de entidades que mais refere a segurança como uma necessidade de reforço de competência das TIC.

Entre as entidades da Administração Pública Central e Regional e Câmaras Municipais, mas também entre as empresas, o tipo de medida de segurança das TIC mais aplicada é a atualização regular do *software*.

Cerca de metade das entidades da Administração Pública Central, em 2019, possuem recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC. Menos de metade das Câmaras Municipais e Administração Pública Regional têm recomendações deste tipo.

O tema mais frequente considerado nestas recomendações, entre as entidades públicas consideradas, é a gestão de níveis de acesso. Nas empresas, é o armazenamento, proteção, acesso e processamento de dados.

CNCS
Centro Nacional de Cibersegurança PORTUGAL

4.
EDUCAÇÃO E SENSIBILIZAÇÃO

Observatório de **Cibersegurança**

A educação e a sensibilização são as áreas que promovem conhecimentos, atitudes e comportamentos, conferindo um grande potencial de proteção à sociedade. Por isso, são aquelas que mais podem contribuir para a correção dos resultados menos positivos em termos de ciber-higiene. São os domínios que têm o poder de fechar o círculo da capacitação, isto é, agir ou reagir relativamente aos diagnósticos sobre a consciência dos cidadãos acerca destas matérias. A "educação" neste contexto engloba os cursos formais, certificados, no âmbito da formação profissional e do ensino superior. A "sensibilização" compreende as ações de consciencialização que procuram promover os comportamentos mais seguros junto de todos os atores sociais, como cidadãos em geral, chefias, trabalhadores ou mesmo profissionais de cibersegurança.

EDUCAÇÃO

Em relação à cibersegurança, os diagnósticos estão feitos. Existe uma significativa falta de profissionais nesta área, quer a nível internacional (TCE, 2019), quer em Portugal (APDSI, 2020). Todavia, nos últimos anos, é possível verificar que existe um aumento no número de cursos e no número de alunos no país. Neste subcapítulo, consideram-se os cursos profissionais não superiores e os cursos superiores registados pelas instituições governamentais ligadas à educação. Sempre que possível, analisam-se os números de inscritos e diplomados, bem como a percentagem de mulheres que frequentam estes cursos, tendo em conta a também diagnosticada sub-representação feminina a este nível (TCE, 2019; CNCS, 2019).

25. Cursos de Especialização Tecnológica, não superiores, de Cibersegurança e Segurança de Informação, em Portugal, divulgados pela DGES em 2020*

Formação	Tipo/Grau	Instituição
Cibersegurança	CET	ATEC - Associação de Formação para a Indústria
Cibersegurança (NOVO)	CET	Centro de Emprego e Formação Profissional de Coimbra
Cibersegurança (NOVO)	CET	Instituto Profissional de Tecnologias Avançadas para a Formação, Lda.
Cibersegurança (NOVO)	CET	NOVOTECNA - Associação para o Desenvolvimento Tecnológico

* A metodologia de recolha dos dados alterou em relação ao ano anterior. Consultar Nota Metodológica.

Tabela 27 | DGES (recolha CNCS)

DESTAQUES

Existem atualmente quatro Cursos de Especialização Tecnológica na área da cibersegurança, sendo que três desses cursos foram registados em 2020.

26. Cursos superiores de Cibersegurança e Segurança de Informação, em Portugal, registados na DGES em 2020. *

Formação	Tipo/Grau	Instituição
Cibersegurança	Curso Técnico Superior Profissional	Instituto Politécnico da Guarda - Escola Superior de Tecnologia e Gestão
Cibersegurança (NOVO)	Curso Técnico Superior Profissional	Instituto Politécnico da Lusofonia - Escola Superior de Engenharia e Tecnologias
Cibersegurança	Curso Técnico Superior Profissional	Instituto Politécnico de Bragança - Escola Superior de Tecnologia e de Gestão de Bragança
Cibersegurança, Redes e Sistemas Informáticos	Curso Técnico Superior Profissional	Instituto Politécnico do Porto - Escola Superior de Tecnologia e Gestão
Cibersegurança, Redes e Sistemas Informáticos	Curso Técnico Superior Profissional	Instituto Politécnico Jean Piaget do Sul - Escola Superior de Tecnologia e Gestão Jean Piaget
Redes e Segurança Informática	Curso Técnico Superior Profissional	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 (NOVO)	Mestrado	Universidade de Aveiro
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

*Não contempla Pós-Graduações.

Tabela 28 | DGES (recolha CNCS)

DESTAQUES

Em relação à edição anterior deste Relatório, foram criados dois cursos em "Cibersegurança": um Curso Técnico Superior Profissional, pelo Instituto Politécnico da Lusofonia, e um Mestrado, pela Universidade de Aveiro;

Ao todo, existem seis Cursos Técnicos Superiores Profissionais, uma Licenciatura, oito Mestrados e um Doutoramento nas áreas de cibersegurança e segurança de informação – portanto, o primeiro ciclo do ensino superior, Licenciatura, é o nível que tem menos cursos nestas áreas, comparativamente.

27. Número de alunos inscritos em cursos superiores de Cibersegurança e Segurança de Informação, em Portugal, registados na DGEEC, 2009-2020.*

	09/10	10/11	11/12	12/13	13/14	14/15	15/16	16/17	17/18	18/19	19/20
TOTAL	27	39	91	98	146	124	243	257	361	509	636
Tendência %	N/A	+44	+133	+8	+49	-15	+96	+6	+40	+41	+25

* Contempla 2 Pós-Graduações: Informações e Segurança (ISCSP-U. Lisboa) e Gestão de Informações e Segurança (ISEGI - U. Nova Lisboa)

Tabela 29 | DGEEC (recolha CNCS)

Total de alunos inscritos em cursos superiores de cibersegurança e segurança de informação, em Portugal, registados na DGEEC, 2009-2019.

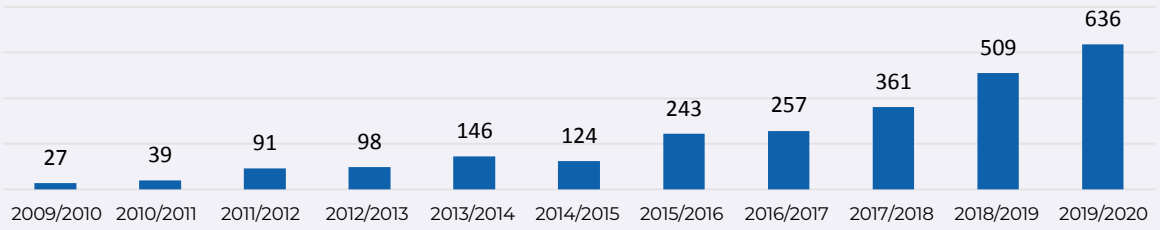


Figura 51 | DGEEC (recolha CNCS)

Percentagem de mulheres inscritas em cursos superiores de cibersegurança e segurança de informação, em Portugal, registados na DGEEC, 2009-2019.

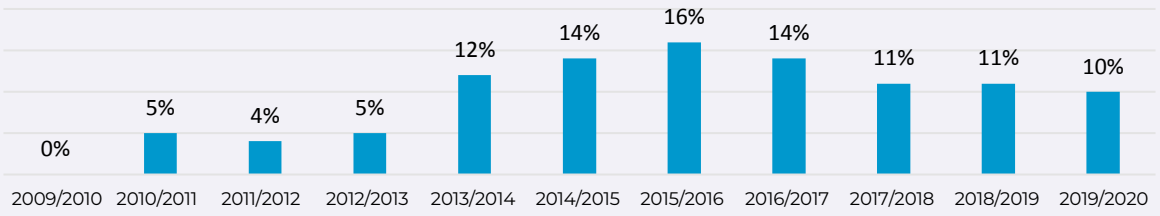


Figura 52 | DGEEC (recolha CNCS)

DESTAQUES

Embora o número de alunos que se inscreveram em cursos superiores de Cibersegurança e Segurança de Informação continue a aumentar de forma contínua desde 2009, com um crescimento de 25% entre o ano letivo de 2018/2019 e o de 2019/2020, a percentagem de mulheres que se inscreveram nesses cursos tem vindo a decrescer desde 2015/2016, atingindo os 10% em 2019/2020, menos 1 pp do que no ano letivo anterior.

28. Número de alunos diplomados em cursos superiores de Cibersegurança e Segurança de Informação, em Portugal, registados na DGEEC, por curso, 2009-2019.*

	09/10	10/11	11/12	12/13	13/14	14/15	15/16	16/17	17/18	18/19	19/20
TOTAL	10	12	10	13	11	38	18	70	361	88	75
Tendência %	N/A	+20	-17	+30	-15	+245	-53	+289	+40	+26	-15

* Existe uma ligeira correção do nº de diplomad0s em 2016/2017 e em 2017/2018 em relação ao Relatório Sociedade 2019.

Tabela 30 | DGEEC (recolha CNCS)

Total de alunos diplomados em cursos superiores de cibersegurança e segurança de informação, em Portugal, registados na DGEEC, 2009-2019.

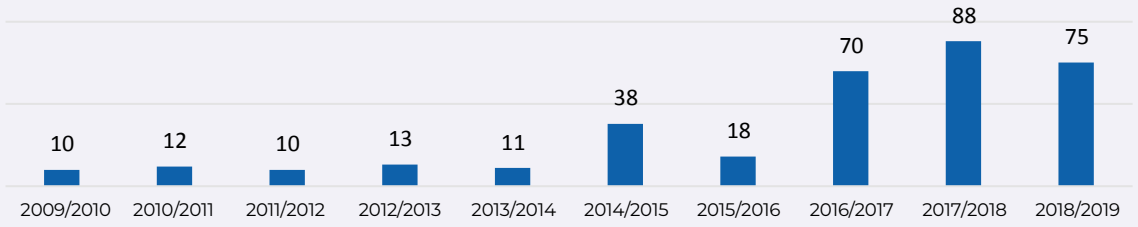


Figura 53 | DGEEC (recolha CNCS)

Percentagem de mulheres diplomadas em cursos superiores de cibersegurança e segurança de informação, em Portugal, registados na DGEEC, 2009-2019.

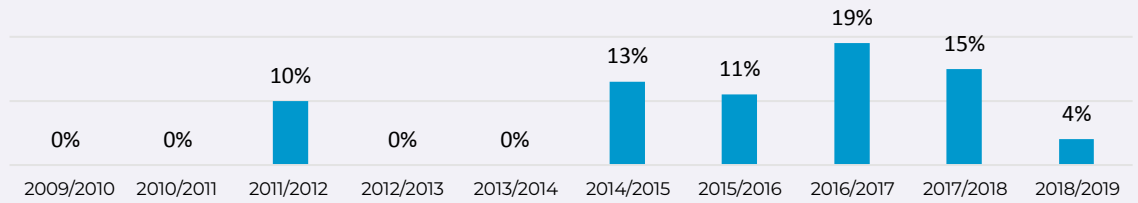


Figura 54 | DGEEC (recolha CNCS)

DESTAQUES

O número de alunos que se diplomaram em cursos superiores de Cibersegurança e Segurança de Informação decresceu 15% no ano letivo 2018/2019, comparando com 2017/2018;

A percentagem de mulheres que se diplomaram em cursos superiores de Cibersegurança e Segurança de Informação decresceu de 15% em 2017/2018 para 4% em 2018/2019.

SENSIBILIZAÇÃO

A sensibilização como atividade responde à necessidade de dotar os cidadãos em geral de competências digitais em cibersegurança. O caráter horizontal do fator humano na cibersegurança (Fovino *et. al*, 2019) faz com que devamos considerar que todos os utilizadores são agentes de segurança das redes e da informação. Portugal continua a apresentar níveis insatisfatórios quanto ao capital humano em termos de digitalização, comparando com a média da UE (CE, 2020), daí que os cursos de caráter mais formal e as ações de sensibilização sejam fundamentais neste domínio, não só para aprofundar os conhecimentos dos especialistas, mas também para disseminar as competências mínimas pelos cidadãos em geral. Um relatório do Oliver Wyman Forum, que apresenta um *Cyber Risk Literacy and Education Index* (OWF, 2020), embora evidenciando como pontos fortes de Portugal a inclusão da população no esforço para a literacia sobre cibersegurança e um foco razoável do sistema educacional nesta literacia, mostra também que há ainda muito por fazer ao nível da motivação da população para as boas práticas. É neste esforço que as ações de sensibilização têm um papel importante.

Neste subcapítulo, apresentam-se os programas de sensibilização considerados mais relevantes, bem como os indicadores quanto a ações de sensibilização junto dos trabalhadores das empresas e da Administração Pública Central e Regional e Câmaras Municipais, fornecidos pelo Eurostat e pela DGEEC, fontes já utilizadas no capítulo anterior.

29. Ações de sensibilização em boas práticas de Cibersegurança e Segurança de Informação, em Portugal, 2019.

Ação	Tipo de Ação	Organização	Sessões realizadas	Pessoas alcançadas
Ações do Centro Internet Segura	Ações de sensibilização *online* e presenciais	Linha Internet Segura, da APAV	4	350
	Ações de sensibilização *online* e presenciais e cursos *online*. Formações de professores creditadas. Campanhas de sensibilização nas Escolas. Iniciativas de Sensibilização Desafios SeguraNet e Líderes Digitais. Integração curricular.	Seguranet e outras atividades, da DGE	220	Cerca de 950 000 (cerca de 6 000 em cursos *online*)
	Ações de sensibilização presenciais	IPDJ	454	12 419
	Ações de sensibilização presenciais e peças de teatro	Fundação Altice	1 862*	70 180*
	Ações de sensibilização presenciais, durante o mês de fevereiro, no âmbito das celebrações do Dia da Internet Mais Segura	Consórcio do Centro Internet Segura e parceiros	**	421 488***
	Ação de sensibilização presencial do Dia da Internet Mais Segura, na Região Autónoma da Madeira	Consórcio do Centro Internet Segura	1	400
Cibersegurança nas PME - A sua empresa está protegida?	Seminários de sensibilização presenciais	IAPMEI	4	139
Eventos, Formação e Programa de Sensibilização em Cibersegurança e Ciberdefesa	Ações de sensibilização *online* e presenciais, Conferências, Seminários, Workshops e cursos de formação	CIIWA	21	2940 (1320 em Simpósio Internacional e Web Summit)
Executive Dialogue on Cybersecurity e COTEC Innovation Summit	Conferências de sensibilização presenciais	COTEC	3	796
Programa de Sensibilização e Treino em Cibersegurança	Ações de sensibilização *online* e presenciais e curso online	CNCS	117	27 842 (18 646 em curso *online*)

* Refere-se ao ano letivo 2018/2019.
** Dados indisponíveis.
*** Parte deste número de pessoas alcançadas pode englobar alguns dos números de pessoas alcançadas indicados pelas outras ações de membros do Consórcio do Centro Internet Segura. Por esta razão optou-se por não apresentar totais de todas as ações. Acresce que os números apresentados no âmbito do Centro Internet Segura ainda não resultam de uma análise exaustiva, pecando por defeito.

Tabela 31 | CNCS e CCIS (entidades referenciadas)

DESTAQUES

As ações realizadas no âmbito do Consórcio Centro Internet Segura atingiram em 2019 mais de 400 mil pessoas;

Apenas dois dos programas identificados, da DGE e do CNCS, integram cursos *online*;

Os programas de sensibilização em Portugal atingem mais de um milhão de indivíduos.

30. Sensibilização dos colaboradores sobre a segurança das TIC nas empresas, em Portugal, 2019. (%)

	Todas		Pequenas		Médias		Grandes	
	PT	UE	PT	UE	PT	UE	PT	UE
Empresas que tornam os colaboradores conscientes das suas obrigações em aspetos relacionados com a segurança das TIC	54	62	50	58	*	78	88	91
Empresas que não tornam os colaboradores conscientes das suas obrigações em aspetos relacionados com a segurança das TIC	45	34	49	38	*	21	12	9
Empresas que tornam os colaboradores conscientes das suas obrigações em aspetos relacionados com a segurança das TIC, através de formação voluntária ou de informação interna disponível (p. ex. informação na intranet)	45	44	40	40	*	61	80	78
Empresas que tornam os colaboradores conscientes das suas obrigações em aspetos relacionados com a segurançadas TIC, através de formação obrigatória ou consultando material obrigatório	27	24	24	21	*	35	54	53
Empresas que tornam os colaboradores conscientes das suas obrigações em aspetos relacionados com a segurança das TIC, através de contrato (p. ex. contrato de trabalho)	27	37	24	34	*	51	53	63

* Dados indisponíveis.

Tabela 32 | Eurostat 2020c

Sensibilização dos colaboradores sobre a segurança das TIC nas empresas, em Portugal. Comparação com a UE. *Todas as empresas.* (%)

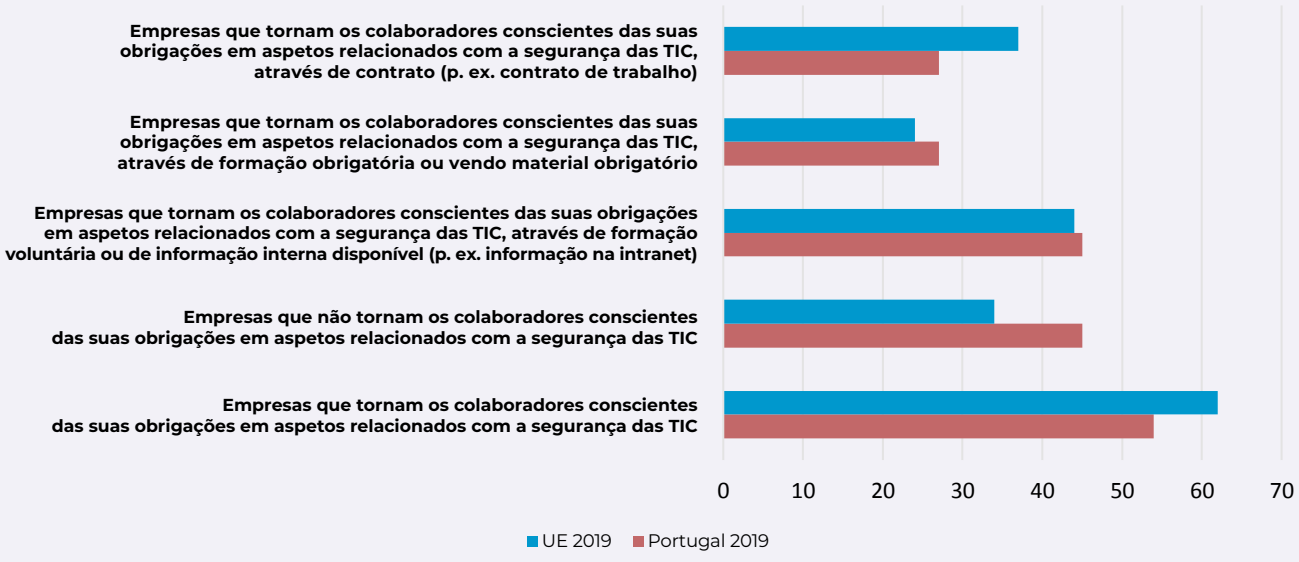


Figura 55 | Eurostat 2020c

Destaques

Existem menos empresas, em Portugal (54%), do que a média da UE (62%) que tornam os colaboradores conscientes das suas obrigações em aspetos relacionados com a segurança das TIC;

As empresas, em Portugal, que o fazem, na sua maioria recorrem a formação voluntária ou informação interna disponível, em 45% dos casos. Apenas 27% recorrem a formação ou materiais obrigatórios. Esta tendência está alinhada com a média da UE;

As grandes empresas são as que mais tornam os colaboradores conscientes das suas obrigações em aspetos relacionados com a segurança das TIC, com 88% em Portugal e 91% na média da UE.

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

	AP Central	AP Açores	AP Madeira	CM
Ações de formação voluntária ou informação interna disponível	63	60	56	58
Ações de formação obrigatória e/ou consulta obrigatória de informação	25	19	18	19
Disposições contratuais	24	13	11	20

Tabela 33 | DGEEC 2020a e 2020b

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

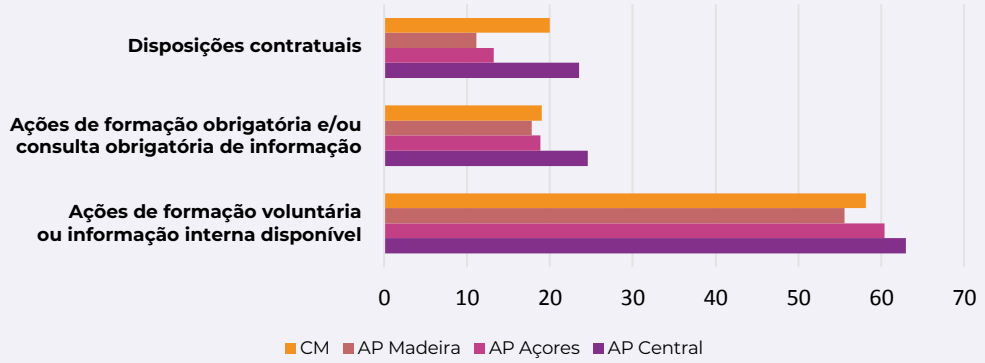


Figura 56 | DGEEC 2020a e 2020b

DESTAQUES

No âmbito da consciencialização das obrigações em matéria de segurança das TIC, a maioria das entidades da Administração Pública Central e Regional e Câmaras Municipais realiza ações de formação voluntárias ou disponibiliza informação interna, com percentagens entre os 56% (AP Madeira) e os 63% (AP Central);

As disposições contratuais são o tipo de ação menos frequente neste âmbito, com valores entre os 11% (AP Madeira) e os 24% (AP Central).

Síntese – A Educação e a Sensibilização, em Portugal, sobre Cibersegurança

Existe um aumento, entre 2019 e 2020, do número de cursos profissionais de Especialização Tecnológica em Cibersegurança.

Também aumentou o número de cursos superiores em Cibersegurança e Segurança de Informação. Não obstante, continua a haver apenas uma licenciatura.

O número de alunos que se inscreveram em cursos superiores de Cibersegurança e Segurança de Informação aumentou em 2019, pelo quinto ano consecutivo.

O número de alunos que se diplomaram em cursos superiores de Cibersegurança e Segurança de Informação decresceu em 2019, comparando com 2018.

A percentagem de mulheres que se inscreveram e diplomaram em cursos superiores de Cibersegurança e Segurança de Informação diminuiu em 2019, em relação a 2018.

Os programas de sensibilização para a Cibersegurança e Segurança de Informação atingem mais de um milhão de indivíduos.

As empresas sensibilizam menos os seus colaboradores do que a média da UE.

A maioria das empresas e das entidades da Administração Pública recorrem a ações de formação voluntária ou disponibilizam informação interna, em lugar de obrigatória.

I. NOTAS CONCLUSIVAS

O *Relatório Cibersegurança em Portugal – Sociedade 2020* procurou este ano desenvolver mais a componente organizacional e disponibilizar uma análise global que permita uma leitura sintética. Como referido, os aspetos mais positivos que os dados apresentados mostram são alguns dos números sobre educação e sensibilização, certos dados absolutos (como os das atitudes e do comportamento organizacional) e o facto de em alguns temas (como os referentes ao comportamento individual) as tendências de evolução serem positivas. Não obstante, verifica-se que os valores em Portugal estão abaixo da média da UE em muitos indicadores. Isto quer dizer que é necessário realizar um esforço acrescido de educação e sensibilização para as atitudes e os comportamentos mais adequados para uma maior proteção dos indivíduos e das organizações.

No Relatório de 2019 identificaram-se alguns riscos em relação ao objetivo de manter a publicação regular deste documento e a comparabilidade internacional dos indicadores. É possível hoje afirmar que em 2020 esses riscos foram mitigados e que se manteve a regularidade e a comparabilidade pretendidas. O lançamento do Eurobarómetro especial 499 assegurou a regularidade dos indicadores. As publicações do Eurostat mantiveram a comparação internacional. Os dados da DGEEC, embora não permitam fazer articulação com a média da UE, são a fonte que mais garantias de regularidade oferece. No Relatório de 2019 também se afirmava ser expectável que houvesse algum dinamismo nos indicadores disponíveis, o que se confirmou, mas no sentido de aumentarem em quantidade e não de diminuírem. A maioria dos indicadores utilizados no primeiro Relatório tiveram continuidade neste.

O objetivo de utilizar estes indicadores para avaliar o impacto da ENSC 2019-2023 ainda não pode ser concretizado no presente documento, na medida em que só será adequado considerar o impacto da ENSC 2019-2023 pelo menos um ano depois do seu início. Os indicadores aqui desenvolvidos referem-se sobretudo a 2019.

J. NOTAS METODOLÓGICAS

Este Relatório recorre a fontes maioritariamente oficiais e consideradas fidedignas enquanto fornecedoras de indicadores viáveis. A metodologia mais frequentemente utilizada pelas diversas fontes é o inquérito por questionário. Não obstante, em vários casos o CNCS produziu os indicadores com base em dados disponíveis ou solicitados às entidades, nomeadamente em grande parte do capítulo sobre educação e sensibilização. O quadro sintético de indicadores proposto é desenvolvido inteiramente pelo CNCS. Trata-se de uma possibilidade de leitura global dos indicadores disponíveis. A virtude desta abordagem prende-se com a possibilidade de sintetizar numa única visão a diversidade de dados. O risco da sua metodologia prende-se com a necessidade de comparar indicadores de fontes diferentes, com bases empíricas diversas e níveis de disponibilidade e de relevância possivelmente díspares. Ao longo do documento, procurou-se ponderar estas situações.

Uma das fontes mais relevantes deste Relatório, tal como em 2019, é o Eurobarómetro, em particular o *Special Eurobarometer 499 Europeans' Attitudes Towards Cyber Security*, mais uma vez na continuidade dos anteriores. Em relação a Portugal, o inquérito deste Eurobarómetro foi realizado pela Marktest – Marketing, Organização e Formação, entre o dia 08/10/2019 e o dia 21/10/2019, a 1007 inquiridos com mais de 15 anos de idade, através de entrevistas presenciais. No conjunto dos países da UE, incluindo o Reino Unido, foram inquiridas 27 607 pessoas.

Os dados do Eurostat relativos a *Perceived barriers to buying/ordering over the internet* (2020a) e a *Safety copies and back up files* (2020b) são recolhidos pelos Institutos Nacionais de Estatística de cada país da UE, INE em Portugal, no âmbito do modelo de questionário sobre o uso das TIC em contexto doméstico e por indivíduos. Em Portugal, as entrevistas foram realizadas de forma mista, recorrendo a inquéritos pela Internet, face-a-face e por telefone, a 6 624 indivíduos com idades compreendidas entre os 14 e os 74 anos, entre o dia 26/04/2019 e o dia 26/07/2019. Ao nível da UE foram inquiridos cerca de 200 mil indivíduos.

No âmbito de *Security policy: measures, risks and staff awareness* (2020c), também do Eurostat, os dados são recolhidos igualmente pelos Institutos Nacionais de Estatística de cada país da UE, INE em Portugal, desta feita através do modelo de questionário sobre o uso das TIC e do comércio eletrónico

em empresas. Em Portugal, o inquérito foi respondido *online* ou através de correio, entre o dia 15/02/2019 e o dia 31/07/2019, abrangendo 7 203 empresas. No total da UE a amostra atinge cerca de 160 mil empresas.

Os IUTIC à Administração Pública Central e Regional e às Câmaras Municipais, da DGEEC (2002a 2002b), são realizados a todo o universo a que se referem em Portugal, através de inquérito preenchido *online*. Aquele que se dirigiu à Administração Pública Central obteve uma taxa de resposta de 99% e os dados foram recolhidos entre outubro de 2019 e março de 2020. O inquérito que incide sobre as Administrações Públicas Regionais obteve uma taxa de resposta de 100% e os dados foram recolhidos entre outubro de 2019 e fevereiro de 2020. Por fim, o inquérito às Câmaras Municipais obteve uma taxa de resposta de 100% e foi realizado entre outubro de 2019 e março de 2020.

No que diz respeito aos dados recolhidos pelo CNCS no capítulo Educação e Sensibilização, os mesmos foram selecionados junto dos *websites* da DGES e da DGEEC, nomeadamente no que se refere aos cursos registados nestas entidades. Quanto aos cursos de Cibersegurança e Segurança de Informação, utilizou-se a mesma metodologia do Relatório de 2019, pesquisando por palavras-chave nos ficheiros disponíveis os cursos e os números de inscritos e diplomados. As palavras-chave utilizadas foram as seguintes: "cibersegurança"; "segurança informática"; "segurança de informação"; "informações e segurança"; verificando-se mais uma vez a presença do termo "segurança" noutros cursos. No que diz respeito aos cursos profissionais, a fonte da informação passou a ser a DGES, o que alterou a lista de cursos apresentados.

Os números relativos à sensibilização resultam de recolha direta junto das entidades mencionadas, com base no quadro de conhecimento sobre as atividades que se estão a realizar, considerando o relacionamento do CNCS e do Centro Internet Segura com os seus *stakeholders*.

Para uma descrição mais detalhada das metodologias utilizadas nos diversos inquéritos, consultar as fontes diretamente, às quais é possível aceder nas referências principais.

K. 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

APDSI - Associação para a Promoção e Desenvolvimento da Sociedade da Informação

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

Fundação Altice

IAPMEI - Agência para a Competitividade e Inovação

IPDJ - Instituto Português do Desporto e Juventude

L. CONSELHO CONSULTIVO DO OBSERVATÓRIO DE CIBERSEGURANÇA

Alexandre Sousa Pinheiro
(Professor Universitário em Direito)

António Brandão Moniz
(Faculdade de Ciências e Tecnologia – Universidade Nova de Lisboa)

José Luís Garcia
(Instituto de Ciências Sociais – Universidade de Lisboa)

Luís Antunes
(Faculdade de Ciências – Universidade do Porto)

Manuel Mira Godinho
(Instituto Superior de Economia e Gestão – Universidade de Lisboa)

Maria Eduarda Gonçalves
(ISCTE – Instituto Universitário de Lisboa)

Paulo Esteves-Veríssimo
(KAUST - King Abdullah University of Science and Technology)

Pedro Miguel Alves Ribeiro Correia
(Instituto Superior de Ciências Sociais e Políticas
– Universidade de Lisboa)

Sandro Miguel Ferreira Mendonça
(ISCTE – Instituto Universitário de Lisboa)

M. REFERÊNCIAS PRINCIPAIS

RELATÓRIOS

CNCS (2020a) *Relatório Cibersegurança em Portugal – Riscos & Conflitos 2020*. Centro Nacional de Cibersegurança.

CNCS (2020b) *Boletim 02/2020*. Centro Nacional de Cibersegurança.

CNCS (2020c) *Boletim 03/2020*. Centro Nacional de Cibersegurança.

CNCS (2020d) *Boletim 04/2020*. Centro Nacional de Cibersegurança.

CNCS (2019a) *Relatório Cibersegurança em Portugal – Sociedade 2019*. Centro Nacional de Cibersegurança.

EC (2020) *Special Eurobarometer 499 Europeans' Attitudes Towards Cyber Security.* European Commission: Brussels. doi:10.2837/672023.

EC (2019) *Special Eurobarometer 480 Europeans' Attitudes Towards Internet Security.* European Commission: Brussels. doi:10.2837/224814.

EC (2017) *Special Eurobarometer 464a Europeans' Attitudes Towards Cyber Security.* European Commission: Brussels. doi:10.2837/82418.

EC (2015) *Special Eurobarometer 423 Cyber Security Report*. European Commission: Brussels. Doi: 10.2837/411118.

EC (2013) *Special Eurobarometer 404 Cyber Security Report*. European Commission: Brussels.

INQUÉRITOS

DGEEC (2020a) *Inquérito à Utilização das Tecnologias da Informação e Comunicação na Administração Pública Central e Regional - IUTICAP 2019.* Direção-Geral de Estatísticas da Educação e Ciência.

DGEEC (2020b) *Inquérito à Utilização das Tecnologias da Informação e Comunicação nas Câmaras Municipais- IUTICCM 2019.* Direção-Geral de Estatísticas da Educação e Ciência.

INQUÉRITOS PARCIAIS

Eurostat (2020a) *Perceived barriers to buying/ordering over the internet*. Code: isoc_ec_inb

Eurostat (2020b) *Safety copies and back up files*. Code: isoc_cisci_f

Eurostat (2020c) *Security policy: measures, risks and staff awareness*. Code: isoc_cisce_ra

OUTROS DOCUMENTOS

ANACOM (2020) *Serviço de Acesso à Internet em Local Fixo: primeiro semestre de 2020*. Autoridade Nacional de Comunicações.

APDSI (2020) *Competências/Qualificações: mapeamento das necessidades de competências na área das TICE visando o ajuste da oferta formativa - estudo exploratório*. APDSI - Associação para a Promoção e Desenvolvimento da Sociedade da Informação.

CE (2020) *Índice de Digitalidade da Economia e da Sociedade (IDES) de 2020, Portugal*. Comissão Europeia.

CE (2017) *Internet Literacy Handbook*. Council of Europe.

CNCS (2019b) *Quadro Nacional de Referência para a Cibersegurança*. Centro Nacional de Cibersegurança.

CNCS (2019c) *Roteiro Para as Capacidades Mínimas em Cibersegurança*. Centro Nacional de Cibersegurança.

ENISA (2017) *Overview of Cybersecurity and Related Terminology*. ENISA-European Union Agency for Cybersecurity.

ENISA (2020) *ENISA Threat Landscape Report 2020*. ENISA-European Union Agency for Cybersecurity.

ENISA (2019) *ENISA Threat Landscape Report 2018*. ENISA-European Union Agency for Cybersecurity.

ISO/IEC 27032 (2012) *Information technology - Security techniques - Guidelines for cybersecurity*. International Standards Organization.

Nai Fovino, I., Neisse, R., Hernandez Ramos, J., Polemi, N., Ruzzante, G., Figwer, M. and Lazari, A., (2019) *A Proposal for a European Cybersecurity Taxonomy*. Publications Office of the European Union, Luxembourg, doi:10.2760/106002 (*online*), JRC118089.

NIST (2017) *Digital Identity Guidelines*. National Institute of Standards and Technology.

OWF (2020) *Global Cyber Risk Literacy and Education Index*. Oliver Wyman Forum.

TCE (2019) *Desafios à eficácia da política de cibersegurança da UE*. Tribunal de Contas Europeu.

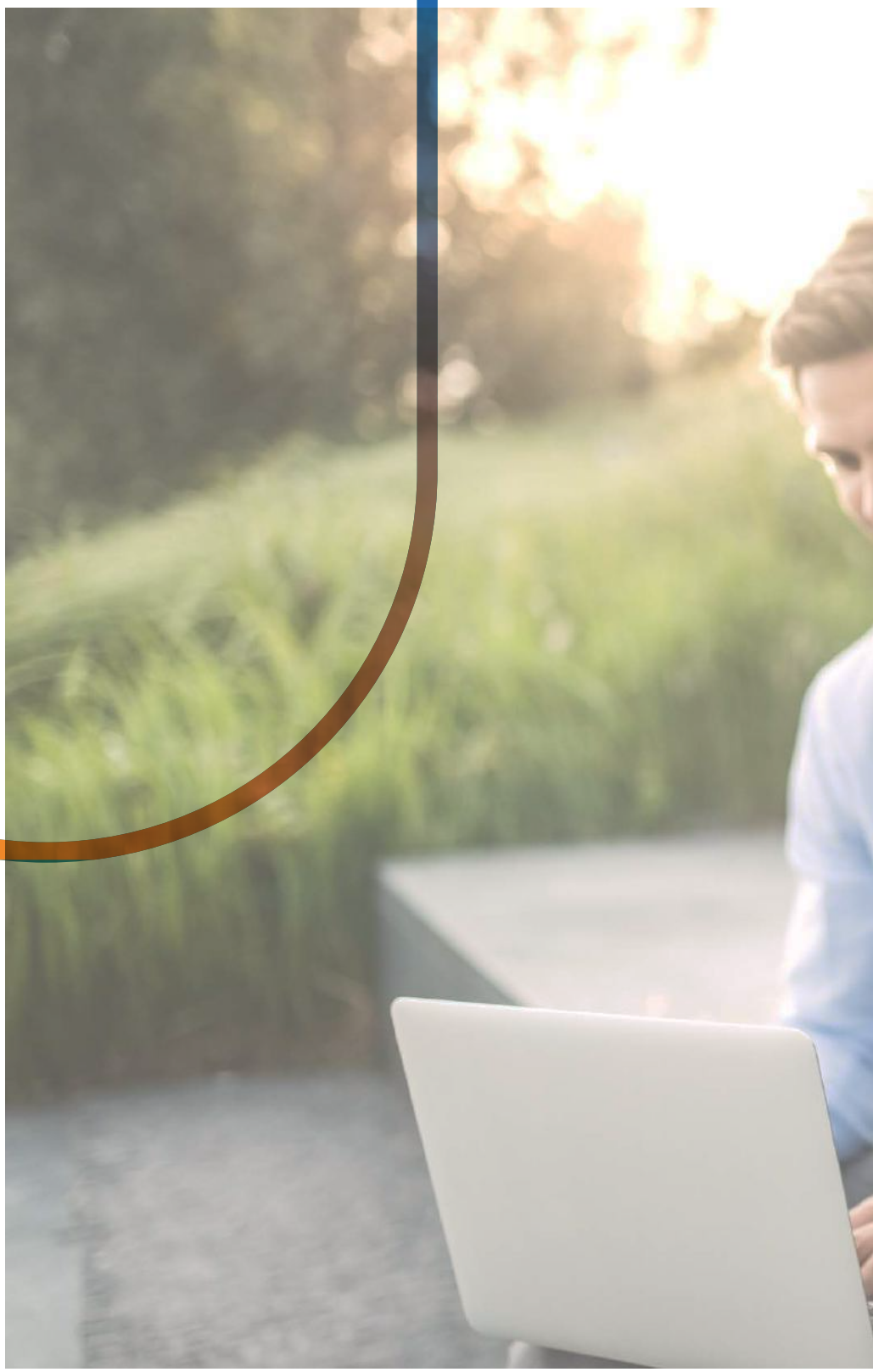
WEBSITES

DGEEC: http://www.dgeec.mec.pt
[última visita a 09/11/2020]

DGES: https://www.dges.gov.pt/pt
[última visita a 09/11/2020]

Estratégia Nacional de Segurança do Ciberespaço 2019-2023: https://dre.pt/home/-/dre/122498962/details/maximized
[última visita a 09/11/2020]

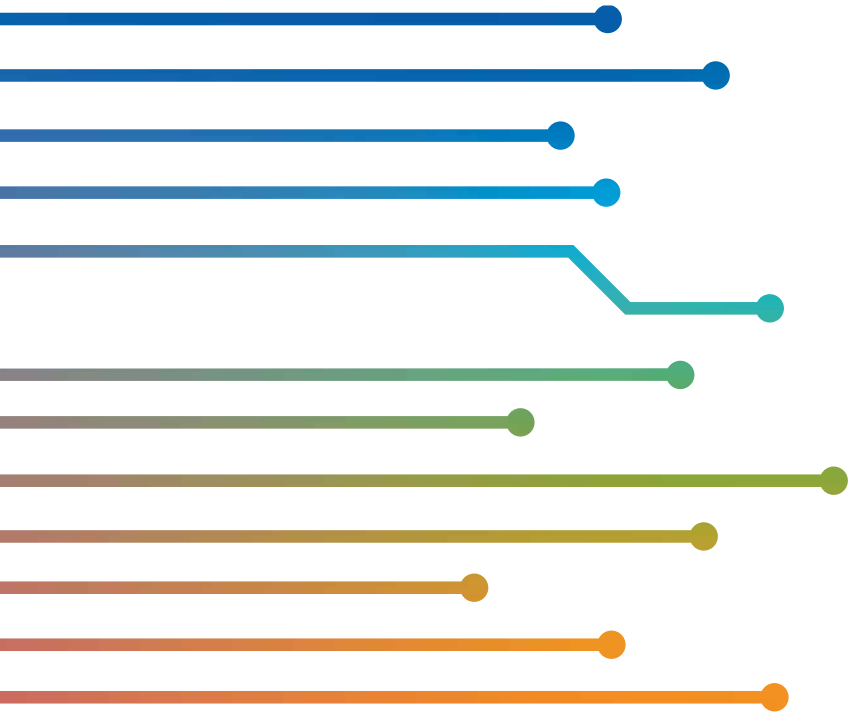
Lei nº 46/2018: https://dre.pt/home/-/dre/116029384/details/maximized
[última visita a 09/11/2020]



CNCS
Centro Nacional de Cibersegurança PORTUGAL

ANEXO
QUADROS SINTÉTICOS DE INDICADORES DETALHADOS

Observatório de **Cibersegurança**



A. ATITUDES – Síntese de Indicadores

Indicador	Absoluto (1) (+50%)	Relativo (1) (+ média UE)	Tendência (1) (positiva)	Pontuação	Observação
1. Preocupações com banco online e compras online (Pelo menos uma preocupação)	+	-	-	1	*Depreende-se, no atual contexto, que ter preocupação é positivo.*
2. Nível de informação (Muito bem ou razoavelmente bem)	-	-	-	0	
3. Concordância com afirmações (Evita revelar informação pessoal online)	+	-	-	0	
4. Preocupações em ser vítima de cibercrime (Média)	+	+	+	3	*Depreende-se, no atual contexto, que ter preocupação é positivo.*
5. Conhecimento de vítimas de ciberameaças	N/A	N/A	N/A	N/A	*Não se aplica devido à ambiguidade deste conhecimento.*
6. Conhecimento de meio de reporte (Pelo menos um)	-	-	N/A	0	
7. O que fariam se fossem vítimas de cibercrime (Média de pelo menos uma ação)	+	-	+	2	
Resultado	4 em 6 (67%)	1 em 6 (17%)	2 em 5 (40%)	7 em 17 (41%)	

Quadro 3

B. COMPORTAMENTOS INDIVIDUAIS – Síntese de Indicadores

Indicador	Absoluto (1) (+50%)	Relativo (1) (+ média UE)	Tendência (1) (positiva)	Pontuação	Observação
8. Alterações de comportamento (Pelo menos uma alteração)	+	-	+	2	
9. Mudança de password (Pelo menos uma mudança)	-	-	+	1	
10. Experiência de vítima de cibercrime	N/A	N/A	N/A	N/A	*Não se aplica devido à ambiguidade desta experiência.*
11. O que fizeram quando foram vítimas de cibercrime (Média de pelo menos uma ação)	+	+	+	3	
12. Reporte de cibercrime (Total de sim)	-	-	N/A	0	
13. O que fazem em relação ao assédio online de crianças (Total algo é feito)	-	-	-	0	
14. Não compraram/ encomendaram online devido a segurança no pagamento	N/A	N/A	N/A	N/A	*Não se aplica devido à ambiguidade desta experiência.*
15. Fazem cópias de segurança (%)	-	-	N/A	0	
Resultado	2 em 6 (33%)	1 em 6 (17%)	3 em 4 (75%)	6 em 16 (38%)	

Quadro 4

C. COMPORTAMENTOS ORGANIZACIONAIS – Síntese de Indicadores

Indicador	Absoluto (1) (+50%)	Relativo (1) (+ média UE)	Tendência (1) (positiva)	Pontuação	Observação
16. Medidas de segurança das TIC nas empresas (Média de medidas todas empresas)	+	+	N/A	2	
17. Política de Segurança das TIC nas Empresas (Total com política de segurança)	-	-	-	0	
18. Empresas que possuem recomendações documentadas (Total com alguma recomendação)	-	-	N/A	0	
19. Realização das atividades relacionadas com a segurança das TIC em empresas	N/A	N/A	N/A	N/A	*Irrelevante para uma valoração a este nível.*
20. Entidades Públicas que têm uma estratégia para a segurança de informação (Média com estratégia)	+	N/A	+	2	
21. Necessidade de reforço de competências TIC em segurança em entidades públicas (Média de entidades com)	+	N/A	-	1	*Neste caso a relação inverte-se: -50% e decrescimento positivos.*
22. Medidas de segurança das TIC utilizadas em entidades públicas (Média de entidades com)	+	N/A	N/A	1	
23. Tipo de pessoal que realizou as atividades de segurança das TIC em Entidades Públicas	N/A	N/A	N/A	N/A	*Irrelevante para uma valoração a este nível.*
24. Entidades Públicas que possuem recomendações documentadas (Média de entidades com recomendações)	-	N/A	N/A	0	
Resultado	4 em 7 (57%)	1 em 3 (33%)	1 em 3 (33%)	6 em 13 (46%)	

Quadro 5

D. EDUCAÇÃO E SENSIBILIZAÇÃO – Síntese de Indicadores

Indicador	Absoluto (1) (+50%)	Relativo (1) (+ média UE)	Tendência (1) (positiva)	Pontuação	Observação
25. Cursos profissionais de Cibersegurança (Nº)	N/A	N/A	+	1	*Sem valor absoluto e sem relação com UE.*
26. Cursos superiores de Cibersegurança e Segurança de Informação (Nº)	N/A	N/A	+	1	*Idem.*
27. Número de alunos inscritos em cursos superiores de Cibersegurança e Segurança de Informação (Nº)	N/A	N/A	+	1	*Idem.*
Mulheres inscritas (%)	N/A	N/A	-	0	*Idem.*
28. Número de alunos diplomados em cursos superiores de Cibersegurança e Segurança de Informação (Nº)	N/A	N/A	-	0	*Idem.*
Mulheres diplomadas (%)	N/A	N/A	-	0	*Idem.*
29. Ações de sensibilização em Cibersegurança e Segurança de Informação	N/A	N/A	N/A	N/A	*Sem valor absoluto, relação com UE ou tendência.*
30. Sensibilização dos colaboradores sobre a segurança das TIC nas empresas	+	-	N/A	1	
31. Sensibilização do pessoal ao serviço sobre a segurança das TIC nas Entidades Públicas	+	N/A	N/A	1	
Resultado	2 em 2 (100%)	0 em 1 (0%)	3 em 6 (50%)	5 em 9 (56%)	

Quadro 6

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**