CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

RELATÓRIO
CIBERSEGURANÇA EM PORTUGAL

ABRIL 2026

SOCIEDADE 2025

7.ª EDIÇÃO

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

ABRIL 2026

RELATÓRIO CIBERSEGURANÇA EM PORTUGAL

SOCIEDADE 2025

7.ª EDIÇÃO

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

FICHA TÉCNICA

Autoria e edição: Centro Nacional de Cibersegurança
Design: Nova Agência
Tiragem: 100 exemplares

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Observatório de Cibersegurança

ÍNDICE

A. ANÁLISE GLOBAL

SUPERFÍCIE DE ATAQUE

COM O AUMENTO SUSTENTADO DA EXPOSIÇÃO DIGITAL DE INDIVÍDUOS E FAMÍLIAS À INTERNET E A CERTOS SERVIÇOS DIGITAIS AUMENTA O RISCO DE CIBERATAQUES, DESTACANDO-SE A ENGENHARIA SOCIAL E A FRAUDE

Na última década, a exposição dos indivíduos e famílias ao digital, incluindo o acesso à Internet e a utilização de alguns serviços digitais relevantes para a cibersegurança não tem cessado de aumentar em Portugal. Porém, tal como ao nível da literacia digital, alguns destes valores ainda se encontram abaixo da média da União Europeia (UE) como, por exemplo, na utilização do *email*, serviços bancários ou compras *online* ou no descarregamento de aplicações por parte dos indivíduos. Por outro lado, os portugueses são, por exemplo, daqueles que mais utilizam as plataformas de mensagens eletrónicas privadas instantâneas na UE. Mantendo-se esta tendência, e apesar dos portugueses se destacarem pela positiva em relação à média da UE em indicadores relativos a implementação de boas práticas e segurança digital, é expectável que o nível de exposição destes últimos aos riscos associados à utilização destes serviços ou aplicações digitais, como o *phishing*, fraudes e burlas *online*, também continue a aumentar.

A ADESÃO AO DIGITAL NAS EMPRESAS PORTUGUESAS TEM VINDO A SER ACOMPANHADA PELA ADOÇÃO DE MEDIDAS DE SEGURANÇA DAS TIC, MAS A SUA MAIORIA AINDA NÃO ATINGIU ELEVADOS NÍVEIS DE MATURIDADE

Verifica-se uma crescente digitalização do tecido empresarial português que acompanha a tendência observada na UE, nomeadamente na disponibilização de acesso à internet aos trabalhadores, na adoção progressiva das tecnologias em nuvem e do trabalho remoto, destacando-se particularmente a disponibilização aos clientes de aplicações móveis por parte das empresas de média e grande dimensão e a adoção da inteligência artificial por estas últimas.

De igual forma, a percentagem de empresas portuguesas que afirmam ter adotado medidas de segurança das TIC tem evoluído positivamente, com especial destaque para os segmentos das empresas de média e grande dimensão. Na implementação de algumas destas medidas, tais como a definição de uma política de segurança para as TIC, a utilização de técnicas de criptografia e a realização testes de segurança, as empresas portuguesas apresentam, pelo menos em 2024, valores acima a média da UE. É, contudo, preocupante constatar que muitas empresas estão ainda longe de aplicar todas as medidas de segurança relevantes para a segurança das TIC como demonstra, por exemplo, a fraca adesão ao múltiplo fator de autenticação, nomeadamente tendo em conta a generalização do trabalho remoto e a ameaça dos *infostealers* e *ransomware* em Portugal.

EMBORA OS PROGRESSOS SIGNIFICATIVOS NA DIGITALIZAÇÃO DA ADMINISTRAÇÃO PÚBLICA TENHAM SIDO ACOMPANHADOS POR UM ELEVADO GRAU DE ADOÇÃO DE MEDIDAS DE SEGURANÇA, ESTAS TÊM-SE REVELADO INSUFICIENTES PARA EVITAR OCORRÊNCIA DE INCIDENTES COM GRANDE IMPACTO NACIONAL

Verifica-se um elevado grau de digitalização dos organismos da administração pública em relação a anos anteriores, nomeadamente em relação à presença destes organismos na Internet, utilização de serviços de pagamentos *online* e implementação de tecnologias emergentes. Todavia, certos indicadores apresentam diferenças importantes entre a administração local e central, destes destaca-se a elevada percentagem de câmaras municipais que disponibilizam aplicações móveis aos cidadãos ou implementam a Internet das Coisas (*Internet of Things* ou IoT).

Apesar do acompanhamento da adoção generalizada de medidas de segurança das TIC na administração pública, por vezes com indicadores bem acima dos observados no setor empresarial, como é o caso da implementação dos mecanismos de autenticação com pelo menos dois fatores, este nível de digitalização revela a existência de uma superfície de ataque ampla que tem vindo a ser explorada, tendo ocorrido vários incidentes e eventos relevantes envolvendo organismos da administração pública em 2024, incluindo casos de *ransomware* e exfiltração de credenciais de acesso ou *login*.

PORTUGAL ENCONTRA-SE LONGE DO GRUPO DE PAÍSES DO ESPAÇO DA UE COM O MAIOR NÚMERO DE ENDEREÇOS DE IP VULNERÁVEIS POR HABITANTE, MAS TAMBÉM LONGE DOS QUE TÊM MENOS VULNERABILIDADES

A exploração de vulnerabilidades foi uma das principais ciberameaças em 2025 e perspetiva-se que continue a ser em 2026, dada a crescente superfície de ataque associada a um aumento no número de dispositivos ligados à Internet, por exemplo na adoção da chamada Internet das Coisas. Entre 2021 e 2025, verificou-se um crescimento de quase 300% no número de notificações recebidas pelo CNCS relativas a sistemas vulneráveis, sendo que muitas das vulnerabilidades associadas a incidentes de segurança podiam ter sido mitigadas. Contudo, e tendo em conta nomeadamente o número de habitantes, Portugal não se destaca no panorama da UE como um país particularmente exposto a vulnerabilidades conhecidas. Ainda assim, verifica-se que duas das cinco vulnerabilidades mais prevalentes no ciberespaço nacional são conhecidas por já terem sido utilizadas em campanhas de *ransomware*.

APESAR DOS AVANÇOS NOS ÚLTIMOS ANOS, A ADOÇÃO DE NORMAS TÉCNICAS E TECNOLOGIAS PARA GARANTIR A SEGURANÇA DA UTILIZAÇÃO DA INTERNET E DO CORREIO ELETRÓNICO AINDA NÃO É COMPLETA EM PORTUGAL, O QUE COMPROMETE A SEGURANÇA DOS UTILIZADORES

Embora o fator humano seja crucial para a segurança *online*, algumas ciberameaças podem ser mitigadas através da implementação de normas técnicas e de tecnologias adequadas, garantindo uma utilização da Internet e do correio eletrónico mais segura e confidencial. Entre estas tecnologias, este relatório identifica uma tendência de crescimento na utilização da versão mais atual do protocolo TLS, essencial para garantir a confidencialidade em páginas de Internet, incluindo pela administração pública central, órgãos de comunicação social e grandes empresas. Contudo, a adoção da tecnologia *Domain Name System Security Extensions* (DNSSEC), importante para garantir a autenticidade das comunicações, ainda é particularmente baixa, verificando-se uma tendência a contraciclo em relação à média da UE.

Portugal acompanha a média da UE na adoção de diferentes protocolos e medidas de segurança das comunicações por correio eletrónico, incluindo uma adoção moderada do *Domain-based Message Authentication, Reporting and Conformance* (DMARC) que tem, no entanto, vindo a aumentar de forma significativa desde 2023. Contudo, é importante salientar que a adesão a medidas de proteção *antiphishing* consideradas no seu conjunto é ainda bastante baixa na administração pública central e em grandes empresas, muitas destas frequentemente utilizadas em ataques de *phishing*.

EMBORA O CRESCENTE RECONHECIMENTO DA IMPORTÂNCIA DA CIBERSEGURANÇA PARA FAZER FACE ÀS CIBERAMEAÇAS SEJA POSITIVO, ESTE NÃO PARECE SER AINDA SUFICIENTE PARA EVITAR IMPACTOS NEGATIVOS NA UTILIZAÇÃO DE PRODUTOS E SERVIÇOS DIGITAIS POR PARTE DOS CIDADÃOS

Em 2024, a cibersegurança recebeu maior cobertura mediática por parte dos órgãos de comunicação social e foi objeto mais frequente de pesquisas em motores de busca por parte dos portugueses. Para além deste aumento relativo à saliência deste tema na sociedade, o tecido empresarial português afirma colocar a cibersegurança num nível de prioridade acima daquele verificado na média da UE.

Ao mesmo tempo, a cibersegurança apresenta-se em Portugal, mais que na média da UE, como um fator importante na decisão dos indivíduos de não utilizarem certos produtos TIC ou serviços digitais, incluindo aqueles disponibilizados pelas entidades da administração pública. Se estes valores parecem indicar que os cidadãos estão cientes da existência de riscos e ameaças na utilização da tecnologia e do ciberespaço, mas podem também revelar um entrave relevante à digitalização na sociedade.

A PERCEÇÃO DE EXPOSIÇÃO A CIBERAMEAÇAS MANTÉM-SE ELEVADA EM PORTUGAL, APESAR DO REFORÇO DAS CAPACIDADES TÉCNICAS E HUMANAS EM CIBERSEGURANÇA, INCLUINDO O RECURSO CRESCENTE A PRESTADORES DE SERVIÇOS PARA COLMATAR DIFICULDADES DE RECRUTAMENTO

Está a aumentar o recurso a prestadores de serviços de cibersegurança externos às empresas e organismos da administração pública, assim como o número de certificações na área de cibersegurança. As empresas privadas são, ainda assim, de longe aquelas que mais recorrem a estes serviços, apresentando valores acima da média da UE. Na administração pública e, em particular nas câmaras municipais, as tarefas de cibersegurança continuam sobretudo a ser prestadas por funcionários do próprio organismo. Em paralelo, nos últimos anos, verifica-se um crescimento sustentado no número de contratos públicos relacionados com a aquisição de serviços e tecnologias de cibersegurança que revela a crescente importância do investimento em cibersegurança na administração pública.

O recrutamento de trabalhadores especializados continua a ser um problema generalizado. Em linha com a média da UE, a cibersegurança ainda é maioritariamente assegurada nas empresas portuguesas por trabalhadores que acumulam essa tarefa com outras funções que não estão diretamente relacionadas e considera-se que é difícil procurar e encontrar candidatos qualificados no mercado para suprir as necessidades. Em Portugal parece existir, contudo, um entrave particular no lado da procura que diz respeito à falta de conhecimento das empresas relativamente às competências necessárias e funções relevantes na área. Estas dificuldades de recrutamento parecem estar a expor particularmente as empresas portuguesas a riscos de cibersegurança, incluindo a níveis acima daquilo que é a perceção média na UE.

AS EMPRESAS E AS UNIVERSIDADES AINDA NÃO APOSTAM, RESPETIVAMENTE, EM AÇÕES DE SENSIBILIZAÇÃO E FORMAÇÃO EM CIBERSEGURANÇA OBRIGATÓRIAS

As ações de sensibilização e formação em cibersegurança são uma das formas mais generalizadas de levar os indivíduos a adotar comportamentos mais seguros na utilização das TIC. Relativamente aos mais de 100 cursos relacionados com a sensibilização para boas práticas de ciber-higiene disponibilizados aos cidadãos pela plataforma NAU, têm vindo a ser emitidos milhares de certificados nos últimos anos, tendo-se assistido a um aumento particularmente pronunciado entre 2023 e 2024. Em Portugal, a percentagem de empresas que promoveram ações de sensibilização também aumentou significativamente desde 2019, mas tanto as entidades públicas como privadas continuam a privilegiar o carácter opcional ou voluntário destas últimas, verificando-se valores abaixo da média da UE.

Apesar de não ser o único percurso possível, a obtenção de capacidades técnicas especializadas também passa, cada vez mais, pelo ensino superior. Ainda assim, em 2025, constata-se a existência de um número ainda muito reduzido de cursos especializados ao nível das licenciaturas e doutoramentos em Portugal, tanto no ensino superior público como privado. Cerca de metade das licenciaturas da área de informática oferecem uma disciplina de cibersegurança, sendo que muitas não exigem aos estudantes a sua frequência obrigatória.

QUAL É O NÍVEL DE PREPARAÇÃO DA SOCIEDADE PORTUGUESA?

B. INTRODUÇÃO

O *Relatório Cibersegurança em Portugal – tema Sociedade 2025* é um documento que tem vindo ser publicado anualmente, desde 2019, com o objetivo analisar as atitudes, os comportamentos, a sensibilização e a educação face à cibersegurança, focando-se, portanto, na componente social deste domínio, incluindo os indivíduos, famílias, empresas e organismos da administração pública. Mantendo a abordagem metodológica que passa pela sistematização e análise de dados disponíveis sobre estas matérias, entre outros, do Eurostat, Eurobarómetro e Direção-Geral de Estatísticas da Educação e Ciência (DGEEC), e recolhendo e produzindo dados próprios, esta edição apresenta algumas novidades.

Apesar de terem sido preservadas a maioria das fontes de dados, procedeu-se, nesta edição, a uma alteração na metodologia de análise, em resultado de um realinhamento do objetivo principal deste relatório, que se foca agora na identificação do estado da resiliência da sociedade portuguesa com base em três dimensões: 1) Riscos de cibersegurança, 2) a superfície de ataque e 3) a ciber-resiliência. Assim, este relatório procurou trazer elementos de resposta à seguinte questão central: Qual o nível de prontidão da sociedade portuguesa (ciber-resiliência) para responder aos vários riscos que se colocam à segurança no ciberespaço (estado da ameaça), que tentam explorar as fragilidades sociotécnicas existentes (superfície de ataque)?

Em relação à primeira dimensão, procede-se a uma análise atualizada dos principais riscos associados às ameaças no ciberespaço de interesse nacional, recorrendo-se para o efeito à análise feita no *Relatório Cibersegurança em Portugal – tema Riscos & Conflitos* (doravante Relatório ReC), publicado em 2025, assim como a fontes alternativas de dados baseadas em inquéritos, em particular aos dados produzidos pelo Eurostat e o Eurobarómetro.

Segue-se um capítulo dedicado à análise da superfície de ataque nacional, com vista a avaliar a existência de fragilidades no ambiente sociotécnico em Portugal passíveis de serem exploradas por cibereameaças. Analisa-se, para este efeito, primeiro a exposição nacional ao digital, uma condição necessária, ainda que não suficiente, para a materialização de riscos de cibersegurança. Existindo exposição ao digital, as segundas linhas de defesa passam pela implementação de medidas organizativas, no caso das organizações, e a adoção de comportamentos seguros por parte dos indivíduos. A exposição ao digital, assim como estas duas dimensões, é analisada, à semelhança de relatórios anteriores, com base em dados de inquéritos produzidos pelo Eurostat, Eurobarómetro e pela DGEEC.

Introduziu-se, nesta edição, também novas análises focadas em fatores técnicos essenciais para analisar a superfície de ataque nacional, nomeadamente a análise da exposição de sistemas de informação nacionais a vulnerabilidades assim como a adoção de normas técnicas, protocolos e outras tecnologias avançadas destinadas a garantir a segurança das comunicações em Portugal, recorrendo-se, para o efeito, a novos dados compilados pelo CNCS e por outras entidades.

Por último, o capítulo dedicado à dimensão da ciber-resiliência analisa a prontidão da sociedade portuguesa para responder a ciberataques, considerando fatores que aumentam a resiliência individual, como o conhecimento de ciberameaças e de boas práticas de ciber-higiene, reforçado através de ações de sensibilização, e organizacional, nomeadamente o investimento na cibersegurança, assim como a formação e capacitação de quadros de cibersegurança. Para esta análise, recorremos a algumas das fontes mencionadas acima, mas também a novos dados recolhidos para esta análise.

Este relatório procurou estabelecer um diálogo, ainda mais próximo que em edições anteriores, com o Relatório ReC. Lidos em conjunto e de forma complementar, estes dois relatórios oferecem uma melhor compreensão do panorama dos riscos no ciberespaço de interesse nacional e da exposição da sociedade portuguesa aos mesmos.

Os relatórios do Observatório do CNCS procuram ser uma fonte privilegiada de conhecimentos e dados científicos disponíveis para apoiar a elaboração de políticas públicas e a tomada de decisão com impacto na segurança do ciberespaço nacional baseada em evidências. Com este panorama mais holístico e integrado da segurança do ciberespaço, ainda que por certo incompleto, deverá contribuir para a identificação e correção de algumas das principais vulnerabilidades atualmente presentes na sociedade portuguesa no domínio da cibersegurança.

EM 2024, 25% DAS CÂMARAS MUNICIPAIS AFIRMAM TER DETETADO INCIDENTES DE CIBERSEGURANÇA

C. ESTADO DA AMEAÇA

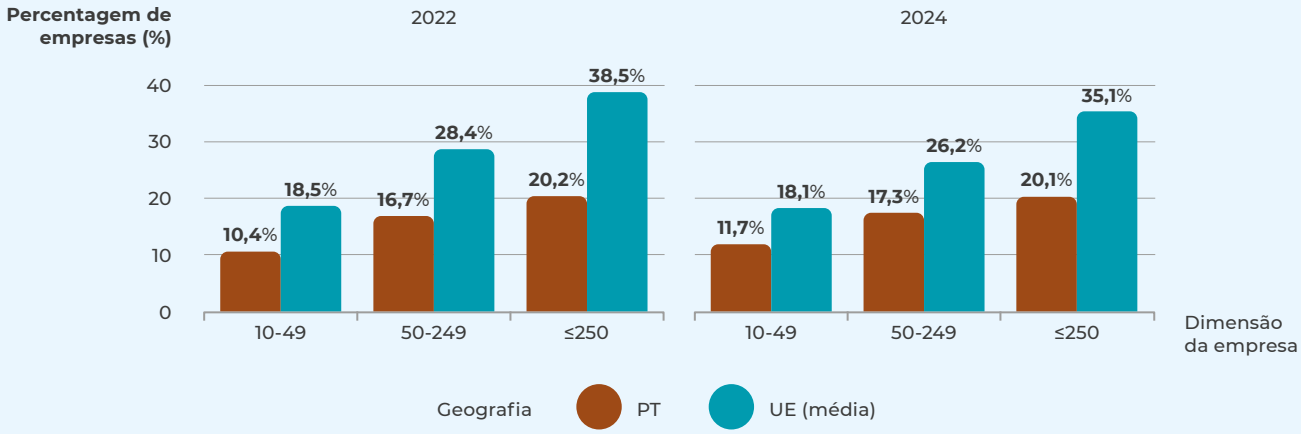
No Relatório ReC, publicado em 2025, foram identificadas a analisadas as ameaças e tendências subjacentes aos incidentes de cibersegurança em Portugal. Em 2024, a equipa nacional de resposta a incidentes de cibersegurança integrada no CNCS, o CERT.PT, registou um aumento de 36% de incidentes de cibersegurança face ao ano anterior. O *phishing/smishing* foi o tipo de incidente mais registado pelo CERT.PT em 2024, seguido da engenharia social e da distribuição de código malicioso *(malware)* em terceiro lugar. Estas três tipologias coincidem com aquelas consideradas mais "ameaçadoras" pelos profissionais em cibersegurança nesse mesmo ano (CNCS, 2025, p. 72, 75). Relativamente ao *phishing/smishing*, é importante referir que as "marcas" mais frequentemente simuladas no conteúdo dos ataques dizem respeito ao setor bancário, seguido dos transportes/logística e serviços de email, destacando-se o grande aumento do uso de "marcas" associadas à administração pública (p. ex. nomes de serviços como a Chave Móvel Digital) (CNCS, 2025, p. 36). Por sua vez, sendo a engenharia social composta por diversos subtipos, destaca-se o aumento do *vishing* e da *CEO Fraud* e, pela primeira vez neste relatório, surgem as técnicas de falso recrutamento. Relativamente à distribuição de código malicioso, o último tipo de incidente deste pódio, é de referir que CNCS tem vindo a detetar um aumento muito significativo de incidentes envolvendo *infostealers*, representando mais de 80% da atividade de *malware* observada no terceiro trimestre de 2025.

Quando considerado o impacto dos incidentes, para além do número de incidentes registados, o Relatório ReC identifica como ciberameaças relevantes em Portugal, para além daquelas referidas acima, o *ransomware*, a exploração de vulnerabilidades e a negação de serviço distribuída *(Distributed Denial of Service ou DDoS)*. Assim, e apesar de se ter verificado uma queda de 35% em 2024, verifica-se que os incidentes de *ransomware* continuam a ter um impacto elevado no ciberespaço de interesse nacional. Desde logo, os três incidentes mais relevantes que tiveram lugar no último trimestre de 2024 configuraram infeções de *ransomware* nas redes e sistemas de informação de entidades da administração pública (CNCS, 2025, p. 11). De igual forma, é importante sublinhar que 45 incidentes estiveram associados à exploração de 36 vulnerabilidades de criticidade alta, não tendo estas sido mitigadas pelas entidades apesar de serem conhecidas há vários anos (CNCS, 2025, p. 43). A relevância dos ataques de DDoS aumentou em 2024, registando-se um tempo médio de indisponibilidade de 8h nos serviços das entidades afetadas por incidentes significativos deste tipo (CNCS, 2025, p. 12).

Para além das entidades nacionais tipicamente referidas no Relatório ReC, o Eurostat também produz dados relativos ao número e impacto dos incidentes de cibersegurança sofridos por empresas, no âmbito do inquérito bi-anual *ICT usage in enterprises* (Eurostat, 2024a). Estes dados permitem-nos, por um lado, analisar o número de incidentes de uma perspetiva comparativa; por outro lado, permite também ter uma visão sobre o número de incidentes sofridos em populações tipicamente fora do âmbito de atividade das entidades nacionais ou para as quais se estima existirem um número relevante de *cifras negras*, nomeadamente por ser menos frequente o reporte de incidentes de cibersegurança às autoridades relevantes.

Figura 1

NÚMERO DE INCIDENTES DE CIBERSEGURANÇA NAS EMPRESAS



Fonte: Eurostat

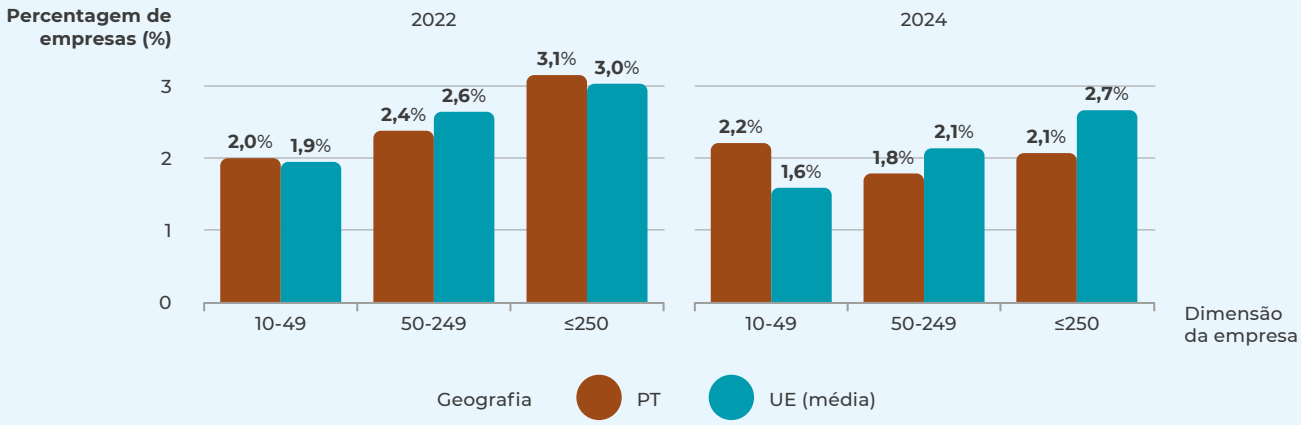
Apesar do aumento de incidentes registado pelo CERT.PT em 2024, olhando para os dados do Eurostat de uma perspetiva comparativa, verificamos que a percentagem de empresas que sofreram incidentes em Portugal, com impacto na disponibilidade de serviços TIC ou que tenham na provocado a destruição ou modificação de dados ou divulgação de dados confidenciais, foi inferior à média da UE. Algo que se verifica em todos os segmentos de dimensão de empresas, categorizadas de acordo com o número de trabalhadores. De facto, quando comparado com os restantes, Portugal parece ter sido dos países em que as empresas menos sofreram incidentes de cibersegurança em 2024, sendo o 5º país com menor percentagem de incidentes de cibersegurança no segmento das empresas com 10-49 trabalhadores (11,72% das empresas), segundo os dados do inquérito *ICT usage in enterprises* do Eurostat. Observa-se, ainda assim, um aumento marginal da percentagem de pequenas e médias empresas portuguesas que sofreram incidentes de 2022 para 2024, sendo que este aumento não se verifica na média da UE com todos os segmentos considerados.

Também o retrato muda ligeiramente quando analisados os incidentes por impacto e causa subjacente. As empresas portuguesas parecem sofrer relativamente mais incidentes que resultam na destruição ou modificação de dados devido a código malicioso ou intrusão, do que a média europeia, em 2024, ainda que a diferença continue a ser marginal.

Apesar da grande maioria dos incidentes de cibersegurança terem lugar em entidades privadas (78%), o Relatório ReC indica que os incidentes nas entidades públicas aumentaram 67% de 2023 para 2024 (CNCS, 2025, p. 26), sendo de destacar o aumento do número destes incidentes nos setores da administração pública local e regional (CNCS, 2025, p. 31). Também de acordo com os dados da DGEEC, entre 2022 e 2024, observou-se um aumento no número de incidentes de cibersegurança na administração pública central/regional e local (DGEEC, 2024a). Este aumento é particularmente substancial no caso das câmaras municipais, onde aumentou 9,4 pontos percentuais (pp), desde 2021, e com 25% dos organismos a reportarem terem detetado incidentes em 2024, quase 6 pp acima da administração pública central/regional.

Figura 2

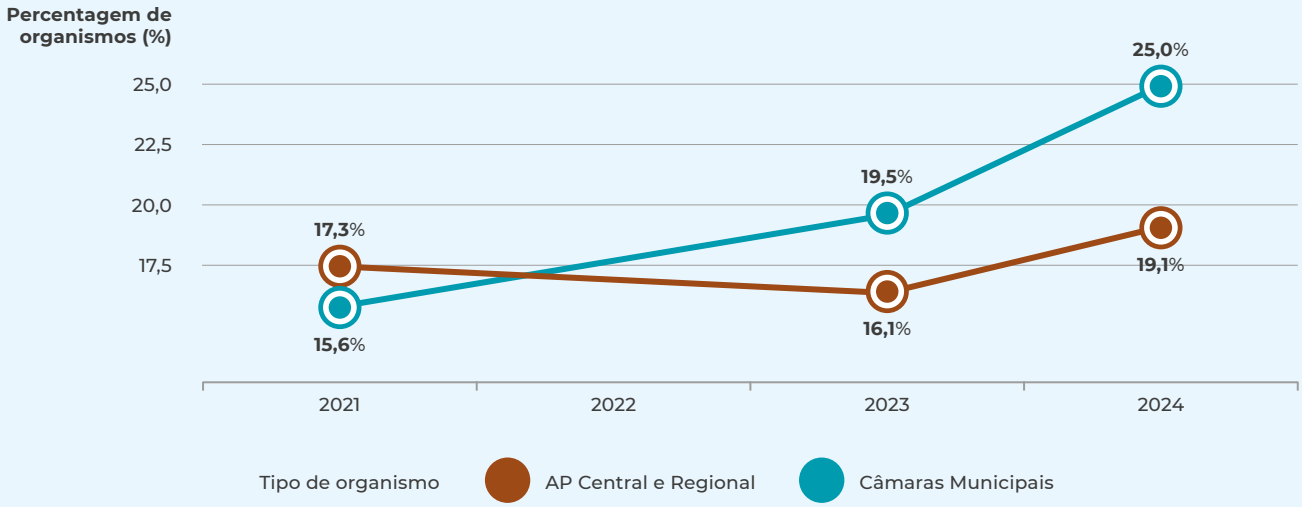
NÚMERO DE INCIDENTES DE DESTRUIÇÃO OU MODIFICAÇÃO DE DADOS NAS EMPRESAS DEVIDO A CÓDIGO MALICIOSO OU INTRUSÃO



Fonte: Eurostat

Figura 3

NÚMERO DE INCIDENTES NA AP

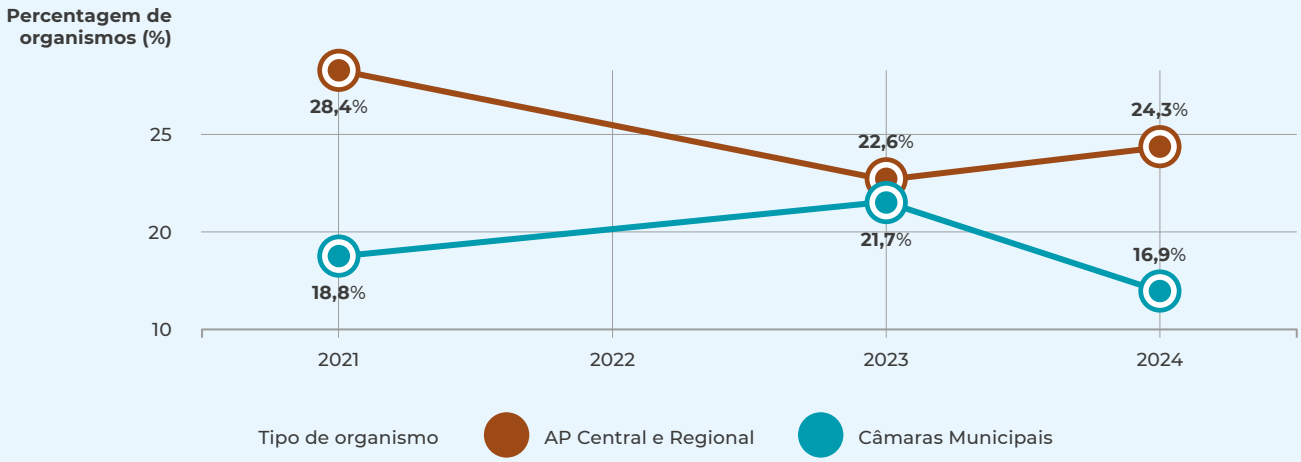


Fonte: DGEEC

Apesar dos organismos municipais terem detetado mais incidentes de cibersegurança que aqueles que pertencem à administração pública central/regional, existe uma maior percentagem destes últimos a reportarem terem sido vítimas de incidentes que provocaram a indisponibilidade dos seus serviços TIC (p. ex. DDoS). Assim, e apesar do número de incidentes deste tipo ser inferior aos experienciados em 2021, 24,3% dos organismos da administração pública central/regional afirmam ter detetado um incidente de indisponibilidade provocado por ação maliciosa em 2024.

Figura 4

INCIDENTES DE INDISPONIBILIDADE POR AÇÃO MALICIOSA

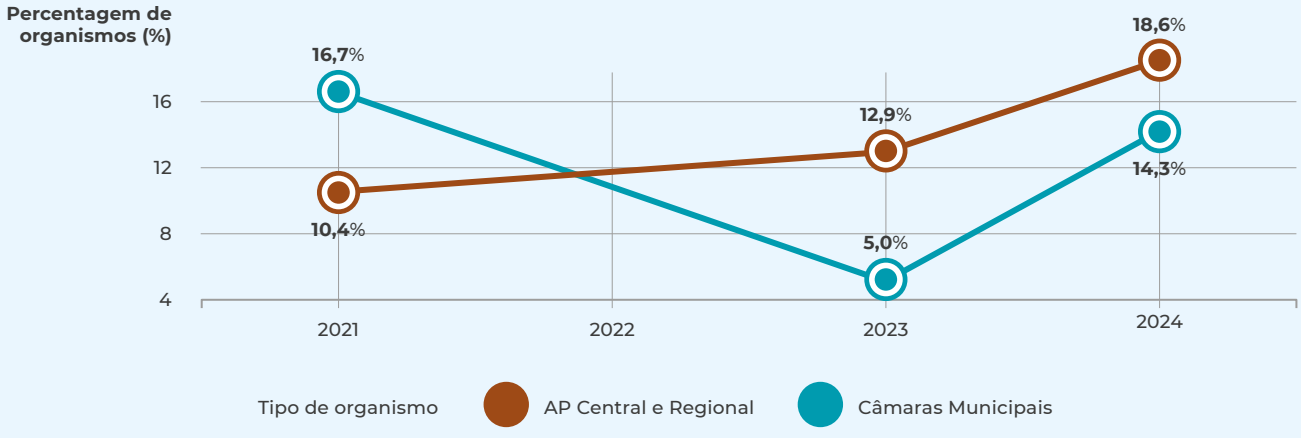


Fonte: DGEEC

Esta diferença entre organismos da administração pública central/regional e municipal pode ser também observada no caso dos incidentes que levaram à destruição ou modificação de dados por ação maliciosa. Resultando de uma tendência crescente desde pelo menos 2021, cerca de 18,6% dos organismos da administração pública central/regional sofreram este tipo de incidentes em 2024. Este valor é superior ao verificado nos organismos municipais (14,3%), ainda que este tenha crescido 9,3 pp relativamente a 2023.

Figura 5

NÚMERO DE INCIDENTES QUE LEVARAM À DESTRUIÇÃO OU MODIFICAÇÃO DE DADOS POR AÇÃO MALICIOSA



Fonte: DGEEC

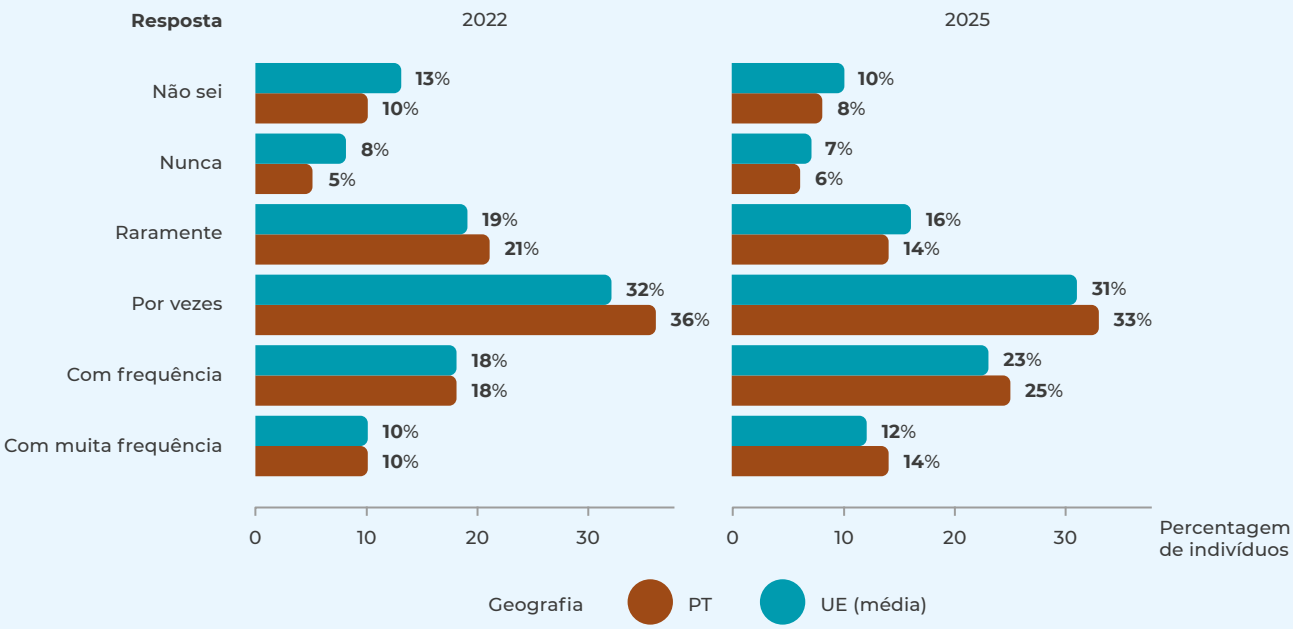
Para perceber o estado da ameaça, o Relatório ReC de 2025 identifica ainda várias tendências com possível impacto no ciberespaço de interesse nacional. Destas destaca-se, em primeiro lugar, o aumento de ciberataques contra as infraestruturas que suportam os serviços de computação em nuvem, visando nomeadamente empresas de telecomunicações e prestadores de serviços de internet. Outra tendência identificada, desde há vários anos, diz respeito à exploração por atores maliciosos de vulnerabilidades em produtos com elementos digitais, que tende a aumentar até pelo número cada vez maior da utilização desses equipamentos em ambiente profissional e doméstico. Uma tendência digna de destaque que, como foi referido, se tem vindo a acentuar desde o início de 2025, é a ameaça dos *infostealers* que recolhem dados sensíveis em dispositivos informáticos, incluindo credenciais de acesso a contas pessoais ou profissionais, dados armazenados nos *browsers* (p. ex. *cookies*, *tokens*, histórico de navegação do utilizador), mas também *emails* e outros documentos. Finalmente, o relatório alerta para os riscos das alterações nas políticas de moderação de conteúdos nas plataformas digitais que favorece a proliferação de desinformação na esfera digital (CNCS, 2025, P. 83-84).

A desinformação é um fenómeno complexo que, em si mesmo, não configura necessariamente um incidente de cibersegurança. Contudo, em diversos contextos, os incidentes de cibersegurança podem potenciar as campanhas de desinformação, nomeadamente através de ações de *hack-and-leak*[1] ou da apropriação de contas *online* de terceiros; por sua vez, as campanhas de desinformação podem, por exemplo, criar narrativas falsas que reforçam o sucesso de ações de engenharia social, incentivar grupos de pessoas a executarem ciberataques contra certos alvos e dificultar a atribuição de um ciberataque. Nesse sentido, e face aos riscos das alterações nas abordagens às políticas de moderação de conteúdos nas plataformas *online*, é importante perceber o nível de exposição dos portugueses a este fenómeno.

Com base em dados do inquérito sobre redes sociais do Eurobarómetro relativos aos anos de 2022 e 2025, analisamos a perceção de exposição à desinformação dos portugueses, em particular as respostas à seguinte questão (Eurobarometer, 2025a): Quão frequentemente considera ter sido pessoalmente exposto a desinformação ou notícias falsas nos últimos 7 dias?

Figura 6

PERCEÇÃO DE EXPOSIÇÃO À DESINFORMAÇÃO



Fonte: eurobarometro social media survey 2025

1 Este tipo de ações envolve a intrusão em redes e sistemas de informação com vista à exfiltração de dados (p. ex. documentos e correspondência eletrónica privada) que são posteriormente disponibilizados publicamente, frequentemente com intenção de influenciar terceiros.

Em Portugal, existe uma percentagem de pessoas que consideram ter sido expostas a desinformação ligeiramente superior à média da UE. Cerca de 14% dos inquiridos consideraram ter sido exposto "com muita frequência" à desinformação, face aos 12% da média da UE, e cerca de 25% e 33%, respetivamente, consideram ter sido expostos "com frequência" ou "por vezes". Em relação a 2022, verifica-se também um aumento no número de portugueses com a perceção de terem sido, recentemente, expostos à desinformação "com muita frequência" (+4 pp) ou "com frequência" (+7 pp), perfazendo um aumento de 11%.

Em comparação, apenas em três Estados-Membros da UE a maioria dos inquiridos afirma ter sido exposto "com muita frequência" ou "com frequência" recentemente a desinformação – Hungria (57%), Roménia (55%) e Espanha (52%) –, enquanto em Portugal esta percentagem ficou pelos 39%, ainda assim o décimo valor mais elevado dos 27. Em todos os Estados-Membros da UE observam-se valores sempre inferiores a um terço dos inquiridos a relatar terem sido "raramente" ou "nunca" terem sido expostos a desinformação e notícias falsas nos últimos sete dias, em particular na França (31%), Alemanha (31%), Chéquia (29%), Finlândia (28%) e Eslováquia (28%).

Analisando os dados de um ponto de vista cronológico, os maiores aumentos percentuais no número de pessoas que considera ter sido exposto a desinformação "com muita frequência" ou "com frequência", relativamente a 2022, ocorreram nos Países Baixos (32%, +19 pp), Dinamarca (35%, +19 pp), Luxemburgo (45%, +18 pp), Malta (45%, +17 pp), Suécia (30%, +14 pp) e Espanha (52%, +13 pp).

A UTILIZAÇÃO DE MULTIPLO FATOR DE AUTENTICAÇÃO NAS EMPRESAS PORTUGUESAS ESTÁ AINDA ABAIXO DA MÉDIA DA UE

D. SUPERFÍCIE DE ATAQUE

Para compreender o grau de exposição da sociedade portuguesa aos riscos e ameaças no ciberespaço, foram analisados dados relativos às dimensões humana e tecnológica da cibersegurança. De facto, ambas as dimensões apresentam aspetos relevantes na identificação de vulnerabilidades suscetíveis de serem exploradas por atores maliciosos na sociedade portuguesa. Estas são por vezes conhecidas na comunidade de cibersegurança como "superfície de ataque", expressão normalmente utilizada em contexto organizacional e aplicado à caracterização das vulnerabilidades técnicas dos equipamentos e serviços que constituem as redes e sistemas de informação[2]. É importante relembrar que nem todas as vulnerabilidades apresentam o mesmo grau de importância e que, numa sociedade democrática, não é razoável esperar que a segurança se imponha, sem ponderação, aos restantes valores com o objetivo de atingir um improvável nível de risco zero.

Este capítulo, que não pode deixar de apresentar apenas uma imagem parcial da realidade, começa por analisar a primeira dimensão olhando para os níveis de utilização das tecnologias digitais e da internet, por parte dos indivíduos, famílias, empresas e organismos da administração pública. Apesar de absolutamente indispensável, a progressiva utilização e integração segura destas tecnologias digitais requer conhecimentos e cuidados particulares. Nesse sentido, procurou-se aferir o nível de competências digitais na utilização destas ferramentas assim como o grau de adoção de boas práticas de medidas de ciber-higiene e medidas organizativas de cibersegurança. No que diz respeito à dimensão tecnológica, procurou-se avaliar, por sua vez, o nível de incidência, *per capita*, das vulnerabilidades técnicas suscetíveis de serem exploradas para fins maliciosos. Outro fator importante nesta dimensão, que tem vindo a ser explorado por atores maliciosos, diz respeito à segurança das comunicações. Em relação ao acesso e utilização segura da internet e mensagens de correio eletrónico, procurou-se comparar o nível de adoção das principais medidas e tecnologias de segurança das comunicações em Portugal em relação a outras geografias.

2 https://csrc.nist.gov/glossary/term/attack_surface

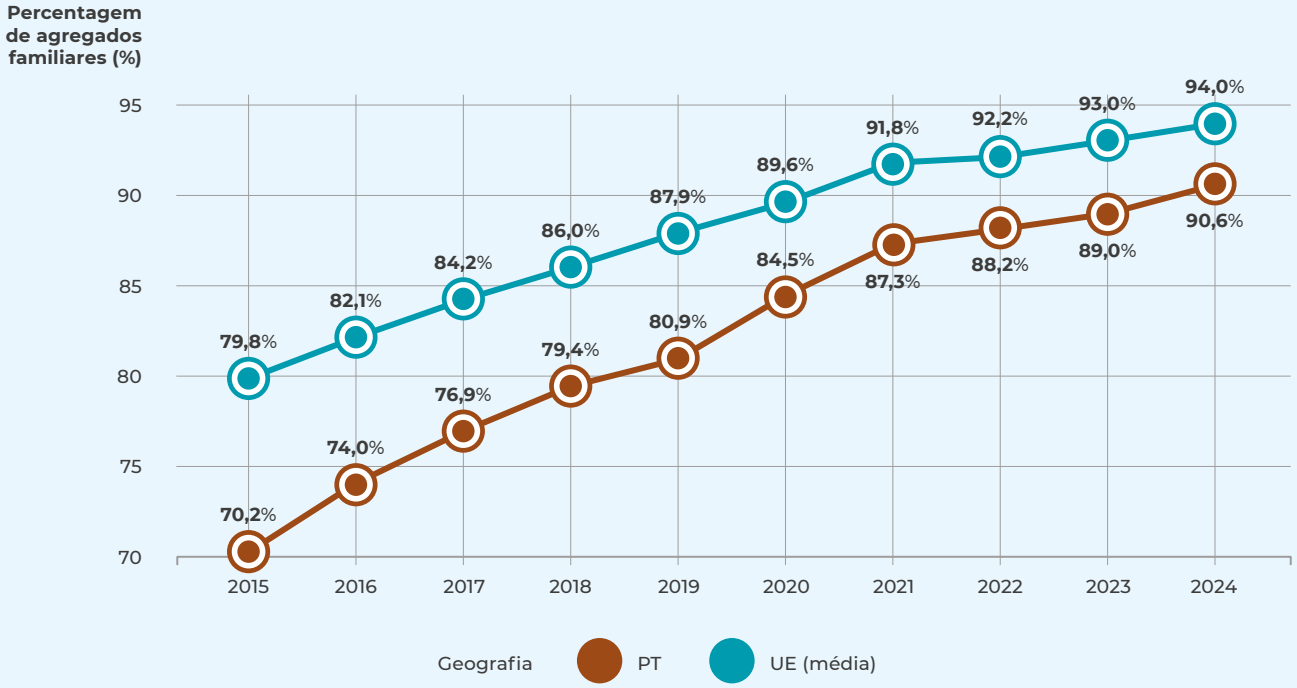
EXPOSIÇÃO AO DIGITAL

ACESSO E UTILIZAÇÃO DA INTERNET POR PARTE DOS INDIVÍDUOS E AGREGADOS FAMILIARES

Acompanhando a tendência que se verifica nos restantes países europeus, o número de agregados familiares com acesso à Internet, em Portugal, aumentou de forma constante durante a última década, de 70,2% em 2015 para 90,6% em 2024, segundo dados do Eurostat (Eurostat, 2024b). Ainda assim, este valor mantém-se abaixo da média da UE, a qual atinge os 94% em 2024.

Figura 7

PERCENTAGEM DE AGREGADOS FAMILIARES COM ACESSO À INTERNET

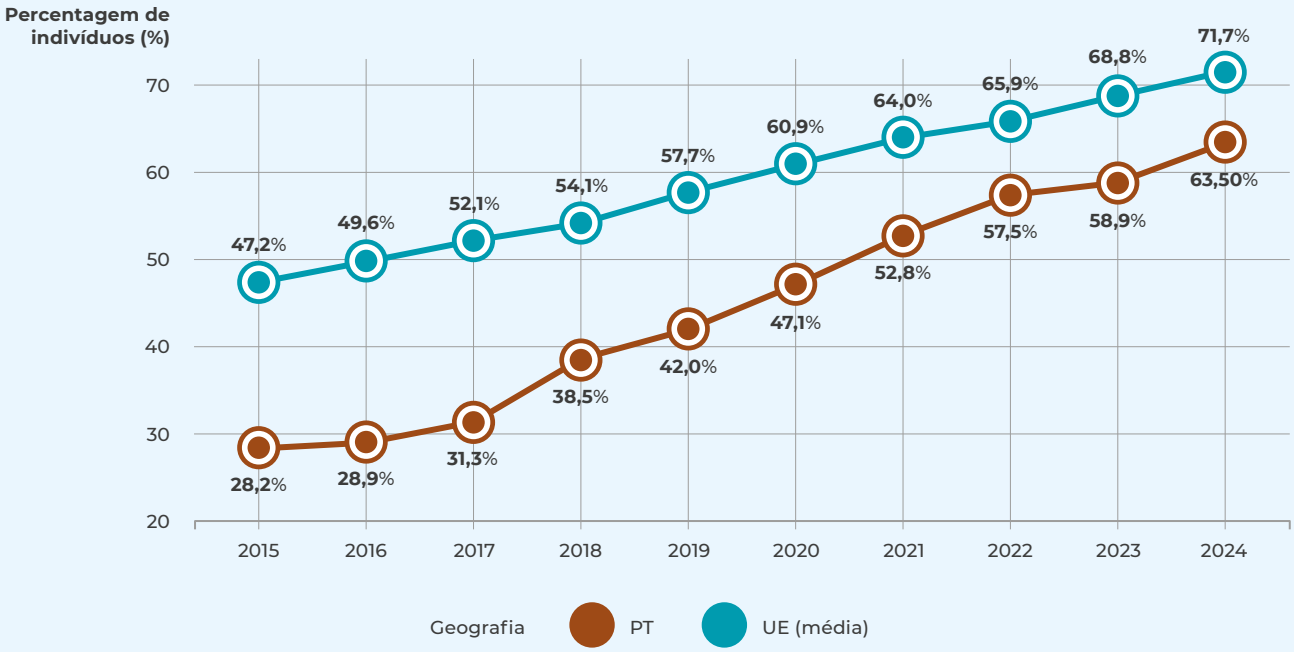


Fonte: Eurostat

Aceder à Internet expõe as famílias e os indivíduos a várias ameaças. Naturalmente, a utilização de alguns tipos de serviços *online*, o acesso ao banco e outros serviços bancários e como as compras, são especialmente visados por cibercriminosos. Como referido anteriormente, o *phishing* e a engenharia social nas suas múltiplas manifestações, tais como a *CEO Fraud*, são uma ameaça frequentemente registada. Curiosamente, em Portugal, o número de indivíduos a utilizar serviços de bancários *online* continua aquém da média europeia (71%) com apenas 63,5% destes a reportarem recorrerem a estes serviços (Eurostat, 2024c). Assim, e se a tendência de crescimento no uso destes serviços se mantiver, é expectável que uma parte ainda muito relevante da sociedade portuguesa possa vir a estar mais exposta a este tipo de ciberameaças nos próximos anos.

Figura 8

PERCENTAGEM DE INDIVÍDUOS QUE UTILIZA SERVIÇOS BANCÁRIOS ONLINE



Fonte: Eurostat

A superfície de ataque para burlas *online* depende também muito dos indivíduos recorrerem à internet para comprar produtos e serviços. De acordo com dados do Eurostat, verificamos a existência de uma tendência nacional crescente, alinhada com a europeia, no uso deste tipo de serviços, de 35,2% em 2020 para 48,9% em 2024 (Eurostat, 2024b). Apesar deste aumento sustentado, Portugal situa-se bem abaixo da média da UE (61,1%) no que diz respeito à utilização da internet por parte dos indivíduos para realizar as suas compras. Como em relação à utilização dos serviços bancários *online*, é possível que nos próximos anos se venha a assistir a um aumento da exposição da população portuguesa a tentativas de burla e fraudes *online*.

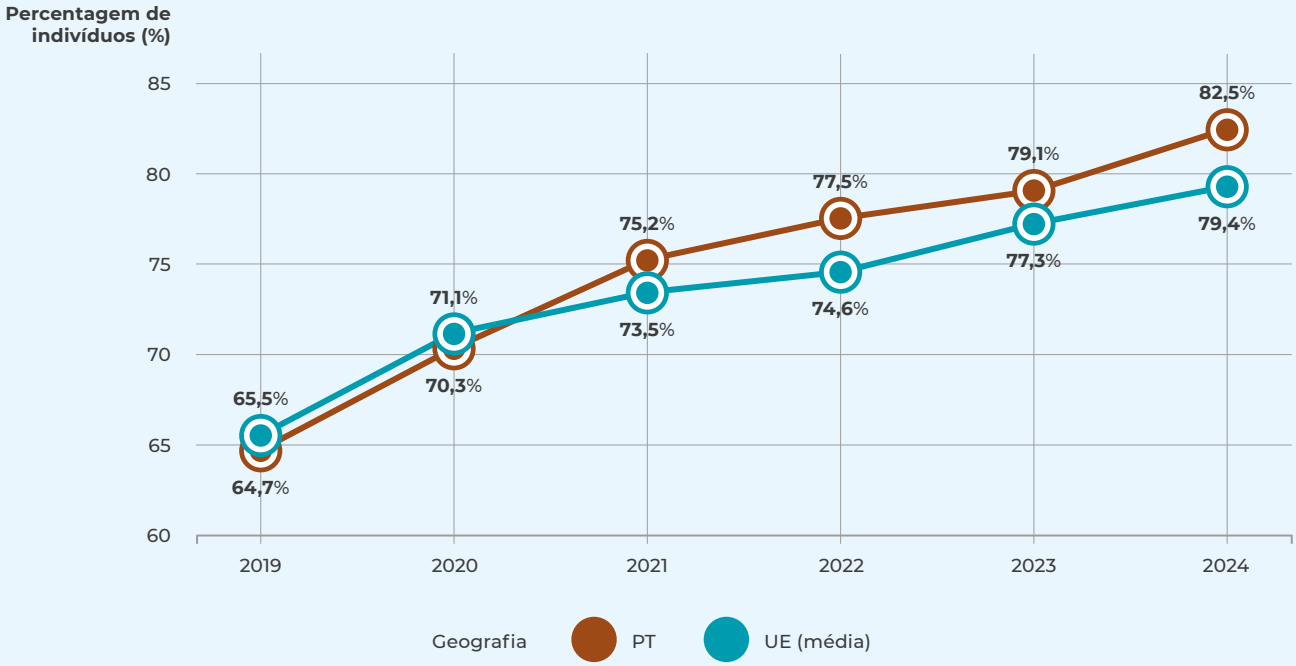
Igualmente relevante para avaliar a superfície de ataque sujeitas a ciberameaças como o *phishing* ou de burlas *online*, como a "Olá Pai, Olá Mãe...", é a utilização do correio eletrónico ou os serviços de mensagens privadas instantâneas (p. ex. Skype, Messenger, WhatsApp). A percentagem de indivíduos a utilizar os serviços de mensagens privadas instantâneas, em 2024, é de 82,5%, um valor acima da média da UE (79,4%). Este valor tem vindo a crescer substancialmente, tanto em Portugal como nos restantes Estados-Membros, sendo que, em 2019, apenas 64,7% e 65.5% dos inquiridos, respetivamente, em Portugal e na UE reportava utilizar estes serviços. A utilização destes serviços mensagens privadas instantâneas conheceu um grande impulso, em Portugal, durante o contexto da pandemia. Os portugueses parecem utilizar, desde esse ano, mais as plataformas de mensagens instantâneas do que o resto da UE. Já a percentagem de indivíduos a utilizar correio eletrónico, em 2024, é de 77% em Portugal, valor 3,5 pp abaixo da média da UE. O número de indivíduos a utilizar correio eletrónico tem observado um aumento quase linear, tendo crescido de 56% em 2015 para os valores atuais, o que representa um aumento de 36%.

ACESSO À INTERNET E À CIBERSEGURANÇA SÃO DIREITOS FUNDAMENTAIS

Aprovada em 2022, a Carta Portuguesa de Direitos Humanos na Era Digital (Lei n.º 27/2021 de 17 de maio) considera a Internet um "instrumento de conquista de liberdade, igualdade e justiça social" assim como um "espaço de promoção, proteção e livre exercício dos direitos humanos, com vista a uma inclusão social em ambiente digital". Vários direitos elencados neste diploma têm relevância para a segurança digital. É o caso, por exemplo, da proibição da interrupção intencional de acesso à Internet (art. 5º), direito à proteção contra a desinformação (artigo 6.º, substancialmente alterado em 2022), direito a comunicar eletronicamente usando a criptografia (art. 8º) ou, ainda, o direito à segurança no ciberespaço através do desenvolvimento de mecanismos que aumentem a segurança no uso da Internet e a promoção de formação, por parte do CNCS, mas também prevenção e neutralização de ameaças à segurança no ciberespaço (art. 15º).

Figura 9

PERCENTAGEM DE INDIVÍDUOS QUE UTILIZA MENSAGENS INSTANTÂNEAS



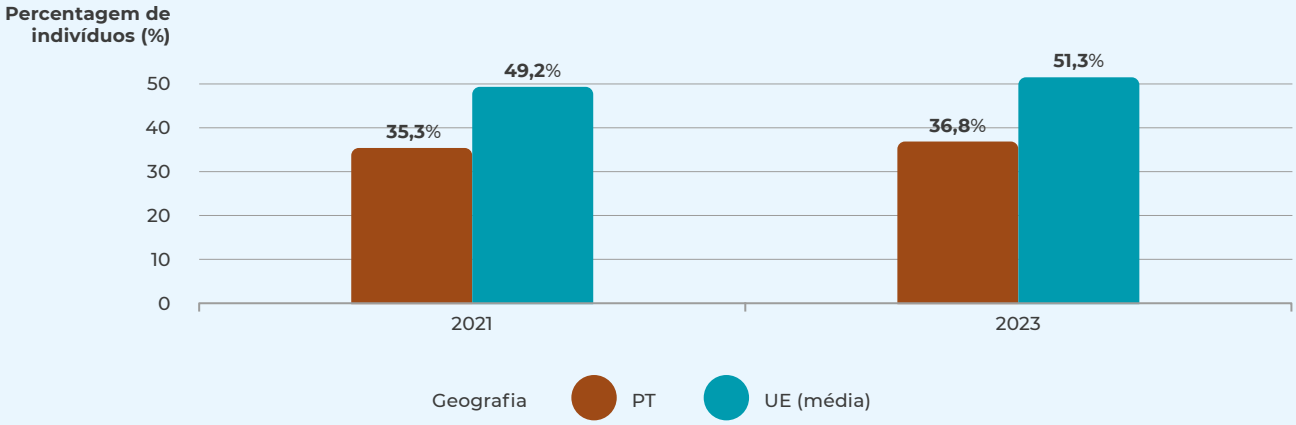
Fonte: Eurostat

A instalação de código malicioso é frequentemente um vetor de acesso inicial para o comprometimento de sistemas (p. ex. computadores, servidores, telemóveis), sendo, por isso, um importante vetor de ataque. Estes ataques ocorrem, por vezes, quando as vítimas são levadas a instalar *trojans*, código malicioso inserido em aplicações com aparência legítima e inofensiva, presentes também em plataformas legitimas que disponibilizam de forma centralizada este tipo de aplicações para dispositivos eletrónicos (p. ex. *Google Play* ou *Apple Store*).

Para analisar a exposição dos indivíduos a estas ameaças, recorremos a dados do inquérito do Eurostat relativo às "Competências digitais" (Eurostat, 2023a), nomeadamente às percentagens estimadas de indivíduos que descarregaram ou instalaram *software* ou outras aplicações nos últimos três meses.

Figura 10

PERCENTAGEM DE INDIVÍDUOS QUE FIZERAM DOWNLOAD DE SOFTWARE OU INSTALARAM UM APLICAÇÃO MÓVEL NOS ÚLTIMOS 3 MESES



Fonte: Eurostat

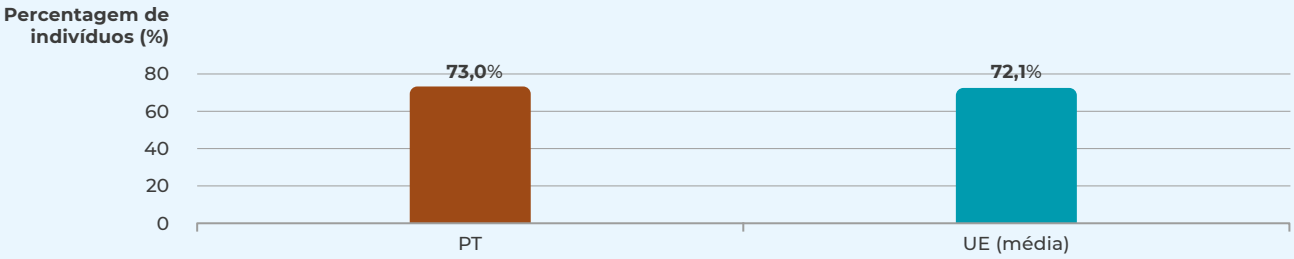
Apenas um terço dos inquiridos em Portugal afirma ter descarregado ou instalado software ou aplicativos nos últimos três meses (36,8%), representado um aumento marginal em relação a 2021 (35,3%). É importante sublinhar que este valor é bastante baixo no contexto da UE, situando-se bem abaixo da média em 2021 e 2023. Portugal é mesmo o 3º país europeu com a menor percentagem, enquanto países como a Finlândia ou os Países Baixos, por exemplo, apresentam valores acima de 70%. Comparativamente, estes números sugerem uma menor exposição da população portuguesa a *software* malicioso que se disfarça de *software* legítimo para ser instalado, como é o caso dos *trojans*. Ainda assim, é importante relembrar que, segundo dados do CERT.PT, variantes deste tipo continuam a ter um peso substancial nas notificações de incidentes relacionados com código malicioso.

A tecnologia da Internet das Coisas, da qual fazem parte os dispositivos conectados que tornam possível as cidades, casas e mobilidade inteligente, assim como a produção industrial moderna, recorre muitas vezes a sensores e outros dispositivos conectados. A proliferação de dispositivos deste tipo levou a um aumento no número de vulnerabilidades. Segundo um estudo de 2023, o número de vulnerabilidades na amostra analisada aumentou aproximadamente 321% entre 2010 e 2022 (Janiszewski et al., 2022) . Um outro estudo identificou, à data de 2025, mais de 23,000 CVEs como sendo associados a tecnologias da IoT (Alsadi et al., 2025). As vulnerabilidades em sistemas da IoT são frequentemente exploradas para fins maliciosos como, por exemplo, a exfiltração de informação sensível e para a criação de *botnets* para a realização de ataques de DDoS. Para além das vulnerabilidades, o código malicioso tornou-se, cada vez mais, uma ameaça relevante para a IoT. A título de exemplo, uma variante de código malicioso infetou mais de 1 milhão de dispositivos em 222 países, em 2025[3]. A percentagem de indivíduos em Portugal que afirma utilizar dispositivos IoT conectados à internet, 73%, está em linha com a média da UE.

3 Ver alerta de código malicioso relativo ao BadBox2.0, emitido pelo CNCS: https://dyn.cncs.gov.pt/pt/alerta-detalhe/art/135938/alerta-de-codigo-malicioso-badbox20.

Figura 11

PERCENTAGEM DE INDIVÍDUOS QUE UTILIZARAM DISPOSITIVOS IOT CONECTADOS À INTERNET



Fonte: Eurostat

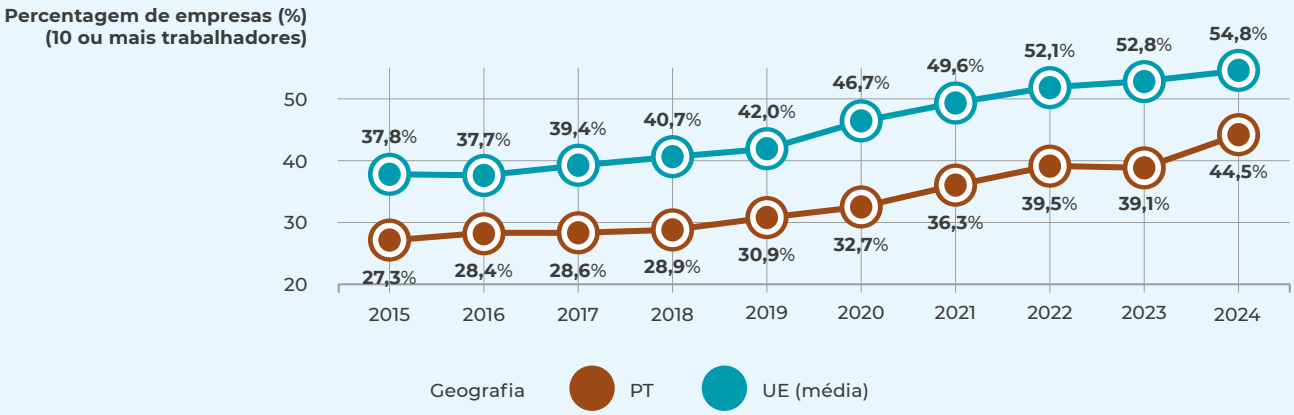
ACESSO E UTILIZAÇÃO DA INTERNET E DAS TECNOLOGIAS EMERGENTES POR PARTE DAS EMPRESAS

É nas empresas e organismos da administração pública que têm lugar os ciberataques de maior impacto para as atividades económicas e sociais. Para identificar a superfície de exposição às ciberameaças destas entidades públicas e privadas, é importante compreender como são utilizadas as TIC e implementadas as medidas técnicas e organizativas de segurança nestas entidades.

Apesar de cerca de 98% das empresas em Portugal, em 2024, estarem conectadas à internet (Eurostat, 2024c), menos de metade concede efetivamente acesso à internet aos seus trabalhadores. De acordo com os dados do Eurostat, em Portugal, a percentagem de empresas, com 10 ou mais trabalhadores, que concede acesso à internet a pelo menos metade dos seus trabalhadores é de 45%, um valor inferior à média da UE (55%). Portugal acompanha, ainda assim, a tendência na UE no que diz respeito ao aumento da percentagem de empresas que concedem acesso à internet aos seus trabalhadores (+17,2 pp em Portugal e +17 pp na UE, entre 2015 e 2024).

Figura 12

PERCENTAGEM DE EMPRESAS (10 OU MAIS TRABALHADORES) QUE CONCEDE ACESSO Á INTERNET A PELO MENOS 50% DOS SEUS TRABALHADORES

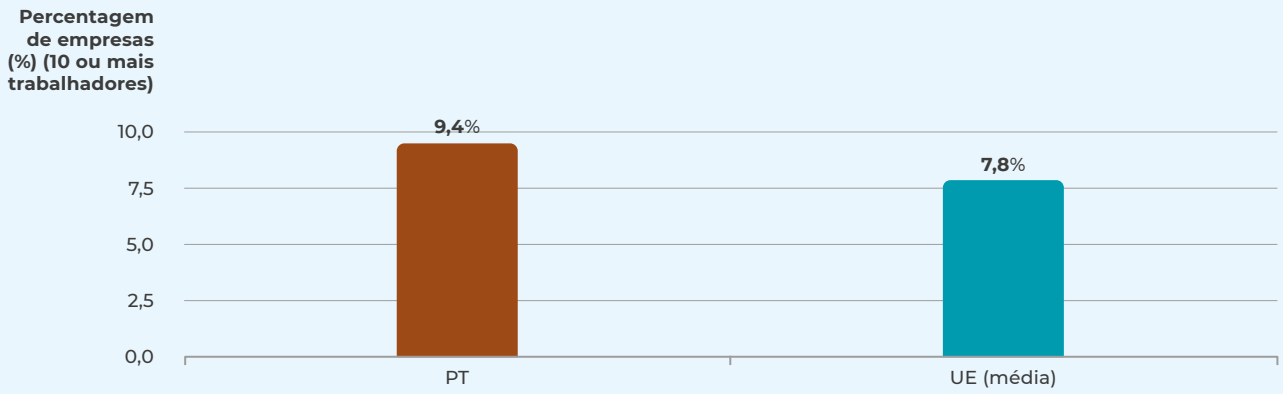


As empresas com páginas na Internet ou com aplicações móveis estão mais expostas a ciberataques. Estes podem ser dirigidos deliberadamente contra as páginas de Internet de determinadas empresas, mas muitas vezes estes ciberataques decorrem na sequência da identificação de vulnerabilidades conhecidas através de *scans* automáticos e aleatórios da Internet. A partir do momento em que estas vulnerabilidades são identificadas, as páginas e aplicações vulneráveis podem ser comprometidas, muitas vezes através da integração de código malicioso com diferentes propósitos. Estes comprometimentos podem ter como objetivo, por exemplo, levar os utilizadores a instalarem aplicações nos seus próprios dipositivos eletrónicos que, por sua vez, passam a poder ser utilizados para outros ataques (p. ex. ataques de DDoS, distribuição de *spam*) sem que o seu proprietário se aperceba.

Considerando apenas empresas com 10 ou mais trabalhadores, de acordo com os dados do Eurostat, observamos que 62% das empresas em Portugal reportava ter uma página na Internet, um valor substancialmente abaixo da média na UE de 76% (Eurostat, 2023b). Já no caso da percentagem de empresas com aplicações móveis disponíveis para clientes, esta parece ser ligeiramente superior nas empresas portuguesas, cerca de 9,4%, relativamente à UE (7,8%).

Figura 13

PERCENTAGEM DE EMPRESAS COM APLICAÇÃO MÓVEL DISPONÍVEL PARA CLIENTES



Fonte: Eurostat

Anteriormente, observámos que Portugal é o terceiro país da UE onde a percentagem de pessoas a afirmar terem descarregado aplicações nos últimos três meses é menor. Igualmente, como veremos abaixo, os portugueses parecem adotar com maior relutância tecnologias da IoT ou recorrer a serviços digitais da administração pública, devido a preocupações relacionadas com segurança. Uma das razões que pode explicar esse comportamento diz respeito ao nível de confiança geral da população em relação a produtos com elementos digitais. Se tanto as páginas de internet e as aplicações móveis apresentam vulnerabilidades suscetíveis de serem exploradas por atacantes, é importante relembrar que estas aplicações requerem muitas vezes o acesso a dados e sensores nos dipositivos móveis para poderem funcionar normalmente. Pela importância crescente que estes dispositivos assumem no nosso dia-a-dia, é fundamental que estas aplicações móveis comerciais tenham em linha de conta a cibersegurança desde a sua conceção e restante ciclo de vida.

PRODUTOS DIGITAIS MENOS VULNERÁVEIS NA UE

O *Cyber Resilience Act* é um regulamento europeu, aplicável a partir de dezembro de 2027, que procura harmonizar as regras de cibersegurança exigidas aos produtos de *software* e *hardware* com elementos digitais que sejam disponibilizados no mercado[4]. As medidas mais relevantes dizem respeito à gestão de vulnerabilidades por parte dos fabricantes, obrigando estes últimos a considerar a cibersegurança durante o ciclo de vida esperado do produto, ou pelo menos cinco anos, evitando, assim, a comercialização de produtos digitais com vulnerabilidades conhecidas. Quando estes estejam a ser comercializados, os fabricantes terão de realizar testes regulares de segurança dos seus produtos, disponibilizando soluções de mitigação para vulnerabilidades identificadas.

A tecnologia em nuvem (*cloud*) é uma das tecnologias emergentes com maior relevância para as empresas. Esta permite, no caso da chamada *cloud* pública, a utilização de recursos e serviços computacionais fornecidos por outras empresas através da internet e sem necessitar de investir em infraestrutura própria dedicada. Para além da redução do custo da infraestrutura e da elevada disponibilidade dos serviços, entre outras vantagens, a adoção desta tecnologia nas empresas facilita também a disponibilização de serviços internos para os trabalhadores em trabalho remoto (CNCS, 2023, p. 17). Isso implica, naturalmente, que as empresas são levadas a exporem as suas redes e serviços internos. Ao mesmo tempo, e atendendo às empresas com relevo mundial no mercado da *cloud* pública, a adoção desta tecnologia significa também que as empresas passam a depender de uma infraestrutura remota para prestar os seus serviços, com servidores que se encontra em geografias onde a legislação oferece menos garantias que aquelas previstas no espaço nacional e da UE em relação à proteção de dados, cibersegurança e, de forma geral, aos princípios do Estado de Direito. Isto é particularmente relevante num contexto em que se observa uma tendência crescente de ataques contra entidades na cadeia de abastecimento digital, com os prestadores de serviços *cloud* a serem frequentemente visados (CNCS, 2024, p. 81; ENISA, 2025, p. 10).

Analisando o número de empresas, com 10 ou mais trabalhadores, a utilizar serviços de computação em nuvem, em particular para o alojamento de bases de dados ou armazenamento de ficheiros. De acordo com os dados do Eurostat, as empresas em Portugal (28,4%) recorrem menos à tecnologia em nuvem que a média da UE (36,1%), apesar de acompanharem a tendência positiva de adoção progressiva desta tecnologia (Eurostat, 2024d).

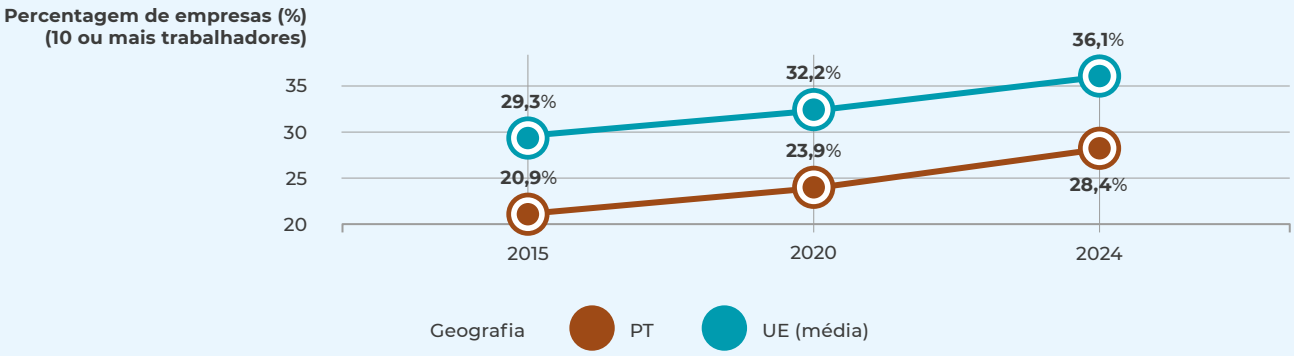
Sem dúvida impulsionado pelo contexto da recente pandemia, o trabalho por acesso remoto tem vindo a generalizar-se nas empresas. De acordo com os dados de um inquérito do Eurostat, em 2024, a maioria das empresas em Portugal, com 10 ou mais trabalhadores, disponibiliza aos seus trabalhadores o acesso remoto ao *email* do trabalho, a documentos ou aplicações (Eurostat, 2024e). Este valor está próximo da média da UE que se situa nos 84% e acentua esta tendência que tem vindo a aumentar tanto em Portugal como no resto da UE desde 2016.

A generalização do trabalho remoto pode resultar, muitas vezes, numa maior diluição da fronteira entre o risco individual e o risco para as empresas. Neste contexto, alguns trabalhadores podem ser levados a utilizar os mesmos dispositivos tanto para o contexto profissional como para fins pessoais. Este fenómeno está relacionado com a tendência, identificada no Relatório ReC de 2025, da crescente ameaça dos *infostealers* e da comercialização das credenciais exfiltradas por este tipo de código malicioso. É importante que todas as entidades, públicas e privadas, em particular aquelas que facilitam o acesso remoto à suas redes e sistemas de informação, estejam cientes dos riscos associados aos *infostealers* e proteger-se contra esta ameaça que potencia outros ciberataques de maior impacto nas redes e sistemas de informação.

4 Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência)

Figura 14

PERCENTAGEM DE EMPRESAS QUE UTILIZOU SERVIÇOS DE COMPUTAÇÃO NA NUVEM PARA HOSPEDAR BASES DE DADOS OU PARA GUARDAR FICHEIROS



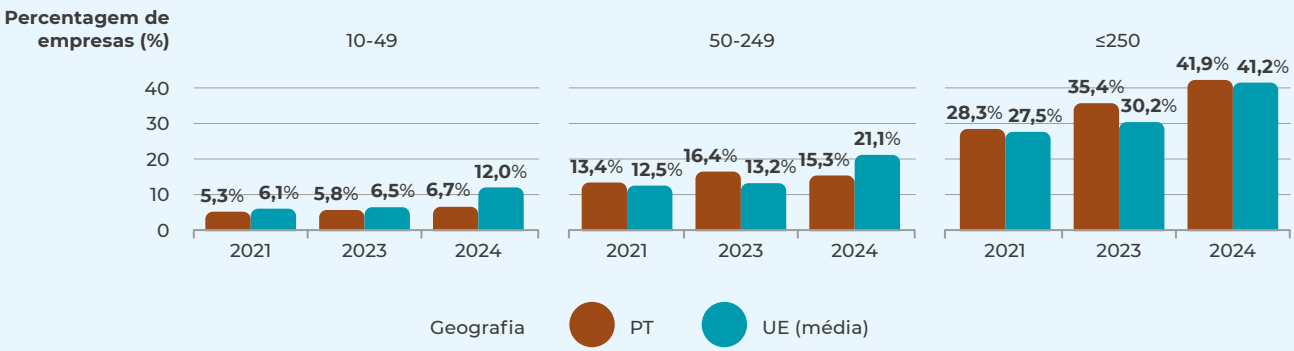
Fonte: Eurostat

Por se tratar de uma outra tendência relevante no Relatório ReC de 2025, é importante considerar a IA na análise da superfície exposta a ciberataques. Embora se discuta a utilização da IA como ferramenta que permite a realização de ciberataques mais eficientes, automatizados e em grande escala e velocidade, por exemplo, através da elaboração de mensagens de *phishing* ou perfis em redes sociais mais convincentes em pouco tempo, é importante não esquecer que as aplicações baseadas em IA, assim como a infraestrutura da qual esta tecnologia depende, também podem ser alvo de ciberataques. Estes podem materializar-se, por exemplo, na "poluição" dos modelos de aprendizagem automática (*Machine Learning*) para fins maliciosos, através da introdução de instruções em ficheiros de configuração de aplicações de IA utilizadas para facilitar o desenvolvimento de *software* por parte dos programadores (ENISA, 2025, p. 14).

Analisando os dados do Eurostat, observa-se uma clara tendência de crescimento na adoção da IA por parte das empresas, independentemente do seu tamanho, tanto em Portugal como na média da UE. No segmento das empresas com 10-49 trabalhadores e 50-249, o crescimento foi mais moderado em Portugal e aquém da média da UE, onde se observou um crescimento significativo. Por outro lado, nas empresas com 250 ou mais trabalhadores, Portugal tem percentagens superiores às da média da UE desde 2021 (Eurostat, 2024f).

Figura 15

PERCENTAGEM DE EMPRESAS A UTILIZAR IA, POR DIMENSÃO



Fonte: Eurostat

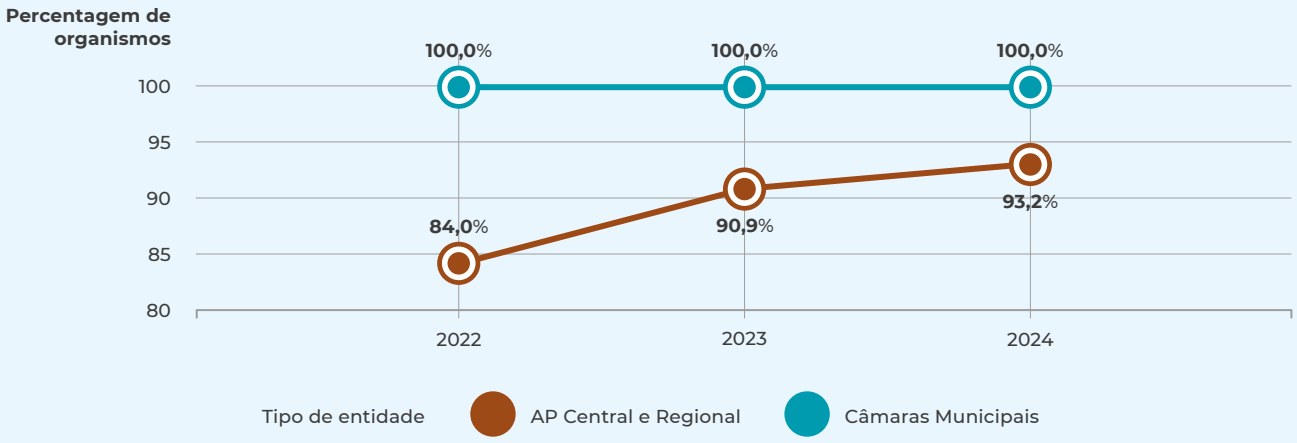
ACESSO E UTILIZAÇÃO DA INTERNET E DAS TECNOLOGIAS EMERGENTES POR PARTE DOS ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA

Segundo o Relatório ReC de 2025, os grupos hacktivistas continuam a ser uma ameaça relevante, recorrendo frequentemente a técnicas disruptivas como a negação de serviços distribuída (DDoS) ou ao *defacement* de páginas de internet (CNCS, 2025, p. 77). Em 2024, 63% dos incidentes de cibersegurança atribuídos a estes grupos ocorreram em entidades públicas dos Estados-Membros, seguindo-se, com 12% dos incidentes, o setor dos transportes, um setor ocasionalmente ligado a entidades de natureza pública (ENISA, 2025, p. 51). Pela natureza política e ideológica da sua atividade, estes grupos tendem a escolher entidades públicas como alvo, colocando frequentemente as páginas destas na primeira linha de ataque.

De acordo com os dados da DGEEC, a quase totalidade dos organismos da administração pública disponibilizam páginas na Internet. No caso das câmaras municipais essa percentagem é de 100% desde 2022, enquanto na administração pública central/regional houve um crescimento sucessivo de 84,0% para 93,2%, entre 2022 e 2024.

Figura 16

PERCENTAGEM DE ORGANISMOS DA AP QUE TÊM WEBSITE



Fonte: DGEEC

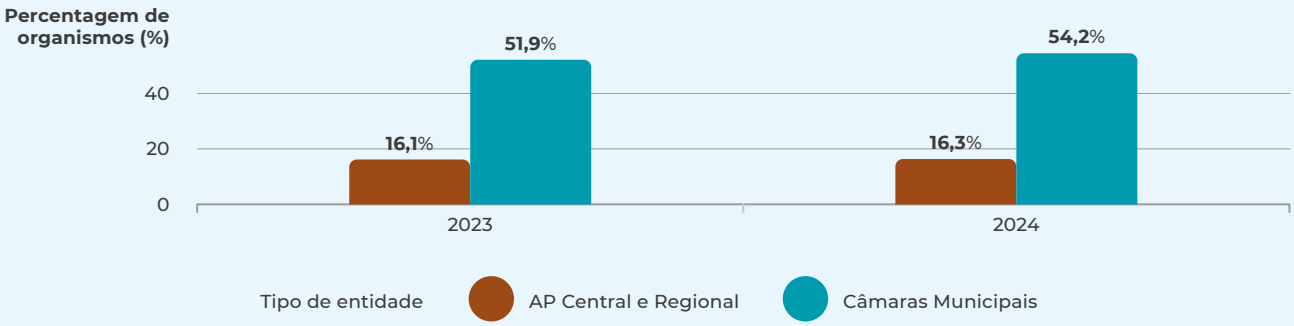
A frequência da disponibilização de aplicações móveis por parte dos organismos da administração pública é mais elevada que aquela observada nas empresas. Verificam-se diferenças significativas também entre os organismos da administração local e administração central e regional, com 54,2% das câmaras municipais a disponibilizar aplicações móveis face a apenas 16,3% por parte dos organismos da administração pública central/regional em 2024.

À sua forte da presença *online* acresce a generalização da utilização de serviços de pagamentos por via digital por parte dos organismos da administração pública. De acordo com os dados da DGEEC, em 2024, cerca de 77% destes organismos da administração pública central/regional, e 68,2% das câmaras municipais efetuaram pagamentos *online*. Isto é particularmente relevante dada a incidência dos ataques de engenharia social em 2024, como a CEO *Fraud*, também na administração pública.

Relativamente ao recurso a infraestruturas *cloud* na administração pública, os dados da DGEEC revelam que a maioria dos organismos adotam estes serviços para, pelo menos, fins de armazenamento de ficheiros. Observa-se, contudo, uma tendência crescente na adoção de serviços de computação em nuvem para hospedar arquivos de banco de dados a nível da administração pública central/regional, com um aumento de 7,9 pp desde 2022, situando-se em 81,2% em 2024. Já nas câmaras municipais, o número de organismos a recorrer a estes serviços desceu de 71,4% em 2022 para 64,6% em 2024. Quando analisamos a adoção de

Figura 17

PERCENTAGEM DE ORGANISMOS DA AP QUE TÊM APLICAÇÃO MÓVEL

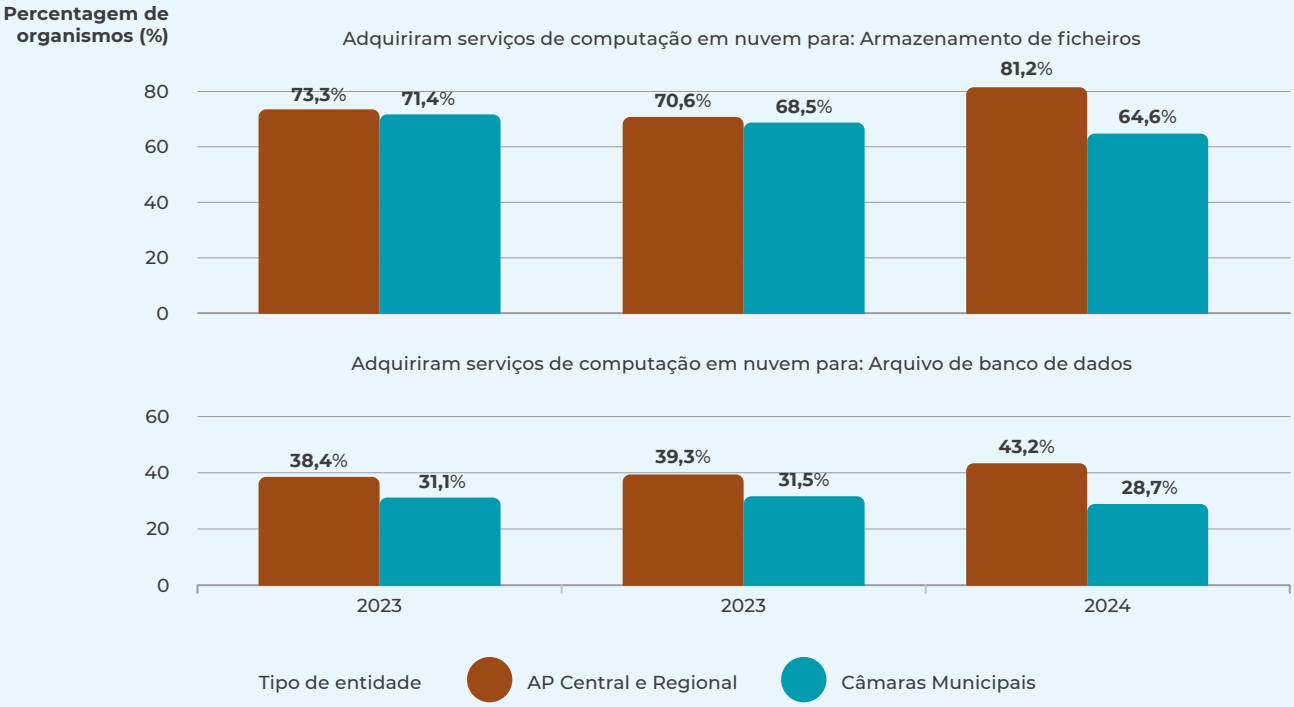


Fonte: Eurostat

serviços deste tipo para hospedar arquivos de bancos de dados, a tendência é a mesma nos dois tipos de entidades públicas, embora com valores inferiores. Na administração central/regional a sua adoção cresce de 2022 para 2024, passando de 38,4% a 43,2%, respetivamente, sendo que nas Câmaras Municipais desce de 31,1% para 28,7% durante o mesmo período.

Figura 18

PERCENTAGEM DE ORGANISMOS DA AP A UTILIZAR SERVIÇOS DE COMPUTAÇÃO EM NUVEM PARA ARQUIVAR BANCOS DE DADOS OU ARMAZENAR FICHEIROS



Fonte: DGEEC

Também em relação à utilização de tecnologias IoT se verifica, uma vez mais, uma grande diferença entre os organismos da administração pública central/regional e as câmaras municipais. Enquanto quase metade destas últimas afirma utilizar esta tecnologia, a percentagem nos organismos da administração pública central/regional fica-se por menos de um terço (24,3%) em 2024.

A adoção da IA na administração pública atinge valores comparáveis aos das empresas com 50 e 249 trabalhadores, com 26% das câmaras municipais e 21,8% dos organismos da administração pública central/regional a utilizarem esta tecnologia emergente em 2024. Embora este valor se tenha mantido relativamente estável no caso dos organismos municipais, estes valores correspondem a um aumento significativo na adoção desta tecnologia na administração pública central/regional relativamente a anos anteriores, quando os valores rodavam apenas os 17%.

Esta análise revela um elevado nível de digitalização dos organismos da administração pública e, em particular, ao nível das câmaras municipais. Estes organismos destacam-se nomeadamente na sua presença na internet, na aposta em aplicações móveis, utilização de tecnologias IoT e IA nos últimos anos. Contudo, esta constatação revela também a existência de uma vasta superfície de ataque que tem vindo a ser explorada, como denota o aumento acentuado no número de incidentes no setor da administração pública local, nomeadamente de 2023 para 2024 (76%), tal como referido no Relatório ReC de 2025.

FATOR HUMANO

ADOÇÃO DE BOAS PRÁTICAS RELACIONADAS COM A PROTEÇÃO DE DADOS

Recorrendo a dados do inquérito do Eurostat relativo à utilização das TIC por parte dos indivíduos e agregados familiares, foi aferida a percentagem de indivíduos que afirmaram ter adotado pelo menos uma das seguintes boas práticas de proteção de dados nos últimos três meses (Eurostat, 2023c):

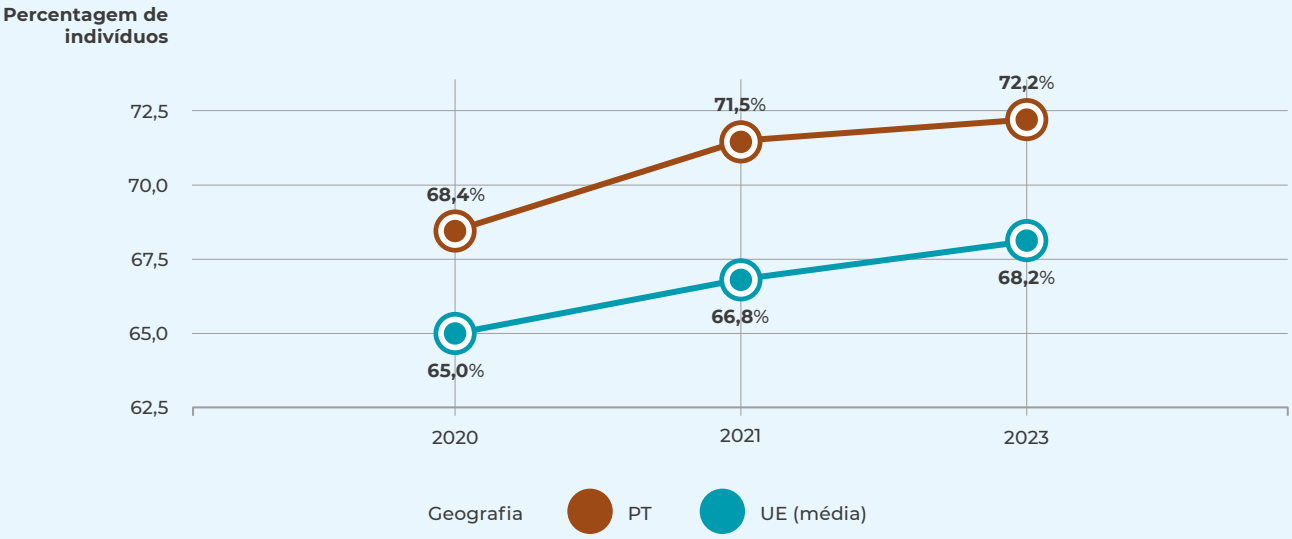
- Verificaram se a página de internet na qual inseriram os seus dados era segura;
- Recusaram autorizar o uso dos seus dados pessoais para fins publicitários;
- Limitaram o acesso ao seu perfil ou respetivo conteúdo nas redes sociais ou em espaço de armazenamento *online*;
- Restringiram ou recusaram o acesso à sua localização geográfica;
- Leram as políticas de privacidade antes de partilharem dados pessoais;
- Questionaram administradores ou prestadores de páginas de internet ou motores de busca para aceder a dados que lhe digam respeito com vista à sua atualização ou eliminação.

De acordo com os dados recolhidos através deste inquérito, em 2023, 72% dos indivíduos em Portugal afirmam terem aplicado, nos últimos três meses, pelo menos uma das seis boas práticas de proteção de dados, elencadas acima, mantendo-se o valor observado em 2021. Este valor situa-se ligeiramente acima da média da UE, de 68% em 2023, apesar desta última ter aumentado 1.4 pp.

Quando estes dados são segmentados por faixa etária verifica-se que 93% dos mais jovens (entre os 16 e 24 anos), em Portugal, dizem adotar pelo menos uma destas boas práticas nos últimos três meses, sendo este um valor substancialmente superior ao da média da UE para este grupo etário (77%). Na faixa etária dos 65 aos 74 anos de idade, a percentagem de indivíduos que afirma adotar pelo menos uma dessas boas práticas, em média, na União Europeia, é superior à portuguesa em 8 pp, ficando esta última nos 35%.

Figura 19

PERCENTAGEM DE INDIVÍDUOS QUE ADOTARAM ALGUMA BOA PRÁTICA DE PROTEÇÃO DE DADOS



Fonte: Eurostat

LITERACIA DIGITAL

A avaliação dos níveis de literacia digital na população, entendida como a "capacidade de aceder, gerir, compreender, integrar, comunicar, avaliar ou criar informação de forma segura e apropriada através de tecnologias digitais" (UNESCO, 2018), é crucial para compreender as potenciais vulnerabilidades decorrentes da interação dos indivíduos com as TIC.

Desde 2021 que o Eurostat procura medir a literacia digital com base num indicador composto por métricas relativas a cinco áreas de competência (Eurostat, 2023d):

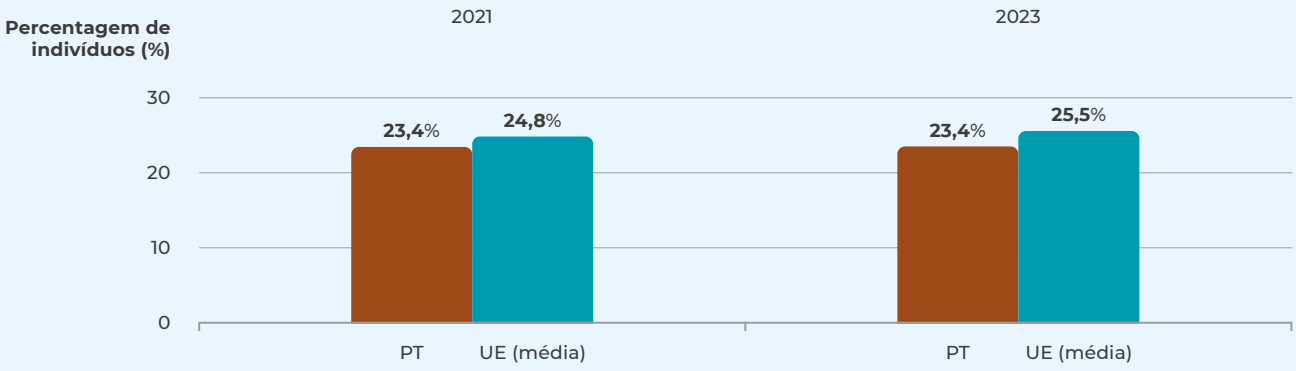
- Literacia de dados e informação;
- Comunicação e colaboração;
- Criação de conteúdos digitais;
- Segurança; e
- Resolução de problemas.

Analisando a percentagem de indivíduos com pelo menos o nível básico no indicador de competências digitais, em 2021 como em 2023, Portugal (56%) parece situar-se ligeiramente abaixo da média da UE (57,6%). Contudo, quando focamos apenas a dimensão "segurança" deste indicador composto, observamos que aproximadamente 72% dos indivíduos em Portugal tem pelo menos o nível básico, enquanto a média da UE se situa 11 pp abaixo.

Para analisar a superfície de ataque relativamente à ameaça da desinformação, olhamos ainda para o indicador da percentagem de indivíduos que verificaram a veracidade de informação ou conteúdo encontrado *online* (incluindo páginas na internet de notícias ou redes sociais) nos últimos três meses (Eurostat, 2023d). De acordo com os dados do inquérito do Eurostat, Portugal está em linha, ainda que ligeiramente abaixo, com a média da UE (25,5%), com cerca 23% dos indivíduos afirmar terem verificado informação ou conteúdos *online* em 2023. Nesse sentido, os portugueses não parecem sentir uma necessidade maior de proceder a uma verificação de conteúdos que a média da UE. Outros Estados-Membros apresentam percentagens de verificação muito mais elevadas, como os Países-Baixos (44%), a Noruega (42%) ou Luxemburgo (40%) em 2023.

Figura 20

PERCENTAGEM DE INDIVÍDUOS QUE VERIFICARAM INFORMAÇÃO IDENTIFICADA ONLINE



Fonte: Eurostat

Assim, não parece existir uma correlação entre a perceção de exposição recente à desinformação na população portuguesa que, como referido anteriormente, apresenta uma percentagem superior à média da UE, e os hábitos de verificação da informação e conteúdos *online*.

MEDIDAS ORGANIZATIVAS

A adoção de medidas de gestão dos riscos de segurança nas redes e sistemas de informação por parte das empresas em diferentes setores críticos da sociedade e economia tem sido um dos pilares fundamentais da legislação nacional e europeia em cibersegurança. A primeira diretiva entrou em vigor em 2016, tendo sido transposta em Portugal nos cinco anos seguintes, e apenas obrigou uma pequena parte das empresas, e somente em alguns setores específicos, a implementarem medidas de cibersegurança. Em 2022, foi publicada uma nova diretiva de cibersegurança que reforça e alarga estas obrigações a mais empresas e setores críticos de atividade, tendo sido transposta para a ordem jurídica nacional com o Decreto-Lei n.º 125/2025, de 4 de dezembro.

Para compreender o estado da adoção de medidas de gestão dos riscos de segurança nas redes e sistemas de informação em Portugal, em comparação com outros países europeus, recorremos aos dados de um inquérito do Eurostat (Eurostat, 2024g) e analisamos, em primeiro lugar, a percentagem de empresas, por tamanho, que adotou pelo menos uma das seguintes medidas de cibersegurança:

- Manter o *software*, incluindo os sistemas operativos, atualizado;
- Monitorização e alerta através de sistema que permite às empresas detetar atividade suspeita nos sistemas TIC, para além de um sistema antivírus tradicional;
- Autenticação de dois fatores, pelo menos (p. ex. palavra-passe de utilizador, palavra-passe de utilização única, código gerado por *token* ou recebido por smartphone, métodos biométricos);
- Implementação de autenticação através de dados biométricos;
- Recolha e arquivo de ficheiros de registo de atividade (*log files*) para análise posterior à ocorrência de incidentes de segurança;
- Gestão dos riscos de segurança das TIC (i.e., avaliação de risco periódica com calculo de probabilidades e consequências potenciais da ocorrência de um incidente de segurança ao nível dos ativos TIC);
- Realização de testes de segurança;
- Implementação de palavras-chave fortes para autenticação;

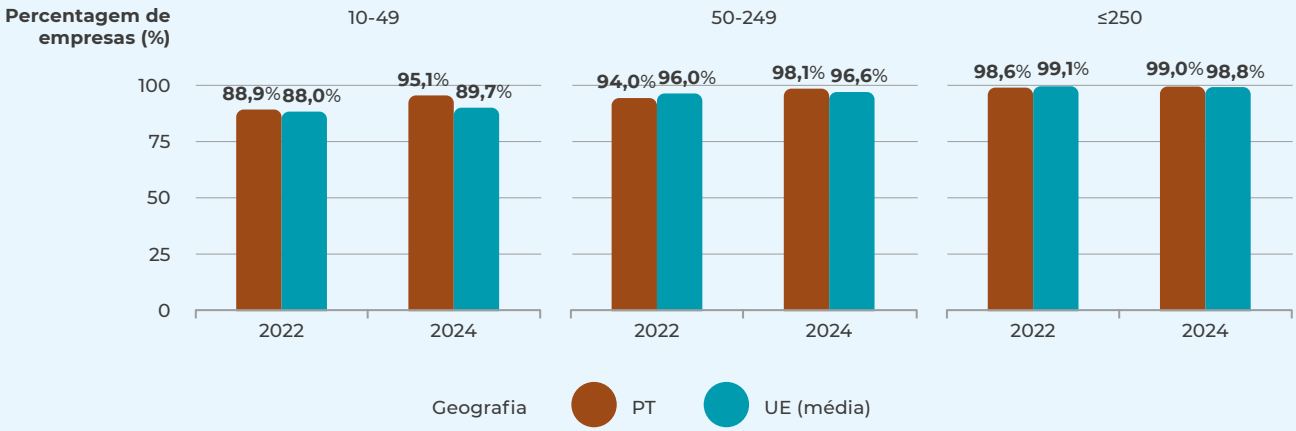
- Utilização de rede privada virtual (*Virtual Private Network ou VPN*);
- Implementação de controlo de acessos dos utilizadores e dispositivos à rede da empresa (*Network Access Control*);
- Guardar cópias de segurança dos dados, incluindo em serviços de nuvem;
- Utilização de técnicas de criptografia para cifrar dados, documentos ou emails.

Nas empresas de pequena dimensão (10-49 trabalhadores), Portugal mostra uma evolução positiva, passando de 88,9% em 2022 para 95,1% em 2024, o que representa um aumento de 6.2 pp na utilização de medidas de cibersegurança, isto é, na implementação pelo menos uma das medidas acima elencadas. Este segmento de empresas em Portugal ultrapassa mesmo a média da UE (89,7%) em 2024, invertendo a situação constatada em 2022, quando se encontrava ligeiramente abaixo (88,9% face a 88,0%).

Nas empresas de dimensão média (20-249 trabalhadores), tanto Portugal como a média da UE apresentam percentagens muito elevadas e próximas entre si, 98,1% e 96,6%, respetivamente, em 2024. Na mesma situação, e sem surpresa, encontram-se as empresas de grande dimensão que apresentam valores que permitem concluir que a quase totalidade das empresas de grande dimensão em Portugal e na UE implementam, pelo menos, uma das medidas de cibersegurança acima referidas.

Figura 21

PERCENTAGEM DE EMPRESAS QUE ADOTARAM ALGUMA MEDIDA DE SEGURANÇA DAS TIC



Fonte: Eurostat

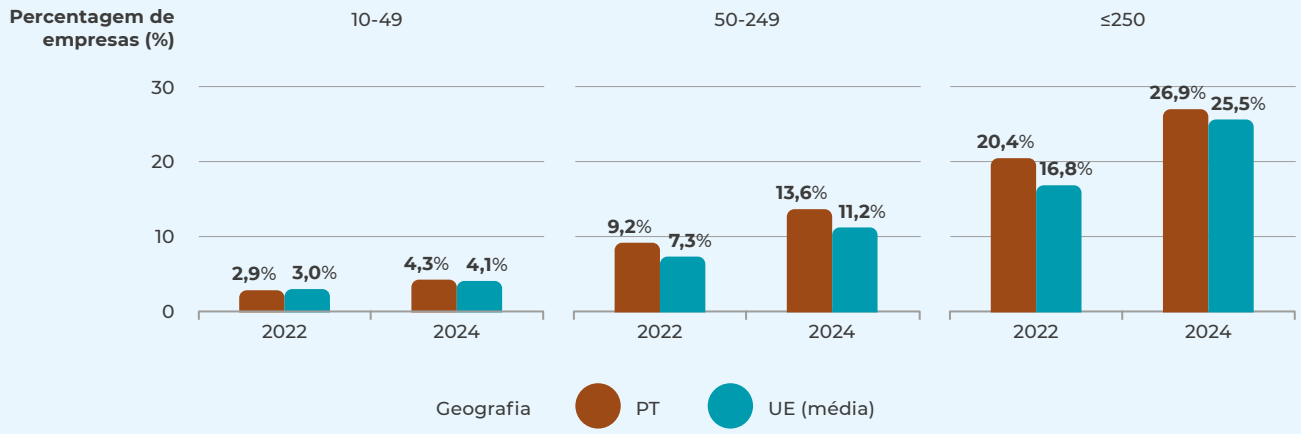
Face a estes valores, é importante referir que as diferentes medidas de segurança elencadas neste inquérito refletem níveis de maturidade em cibersegurança muito distintos. Por exemplo, enquanto a existência de uma política de utilização de palavras-chave forte constitui uma medida recomendada a qualquer empresa, a realização de avaliações de risco periódicas em relação aos ativos críticos exige um nível de recursos humanos e financeiros que não estão disponíveis a todas as empresas.

De novo, o panorama muda de forma radical quando analisamos as percentagens relativas à adoção de todas as medidas de segurança elencadas no inquérito; observa-se uma redução drástica dos valores em todos os segmentos de empresas, tanto em Portugal como na média da UE, em qualquer período considerado.

Ainda considerando a adoção de todas as medidas de segurança referidas no inquérito, observamos que as percentagens relativas às pequenas empresas em Portugal acompanham a média da UE, respetivamente, 2,9% e 3.0% em 2022 e 4,3% e 4,1% em 2024. É importante sublinhar, no entanto, que em igual período, Portugal destaca-se da média da UE pela positiva, tanto no segmento das empresas de média dimensão como no segmento das empresas de grande dimensão, ainda que de forma mais ligeira em 2024. Embora estes valores sejam relativamente baixos, a tendência temporal é de uma evolução positiva com a percentagem a aumentar 4,4 pp nas empresas de média dimensão, entre 2022 e 2024, e 6,5 pp nas empresas de grande dimensão em Portugal.

Figura 22

PERCENTAGEM DE EMPRESAS QUE ADOTARAM TODAS AS MEDIDAS DE SEGURANÇA DAS TIC ELENCADAS



Fonte: Eurostat

Quando analisada a implementação individual destas e outras medidas de segurança relevantes, verifica-se um aumento significativo na percentagem de empresas, com mais de 10 trabalhadores, com política de segurança para as TIC definida e revista nos últimos 24 meses, passando de 29% em 2015 para 42% em 2024, representado um aumento de 12,7 pp. É de sublinhar que, com exceção de 2019, Portugal esteve sempre acima da média da UE neste indicador, sendo que esta última tem evoluído em contraciclo desde 2022.

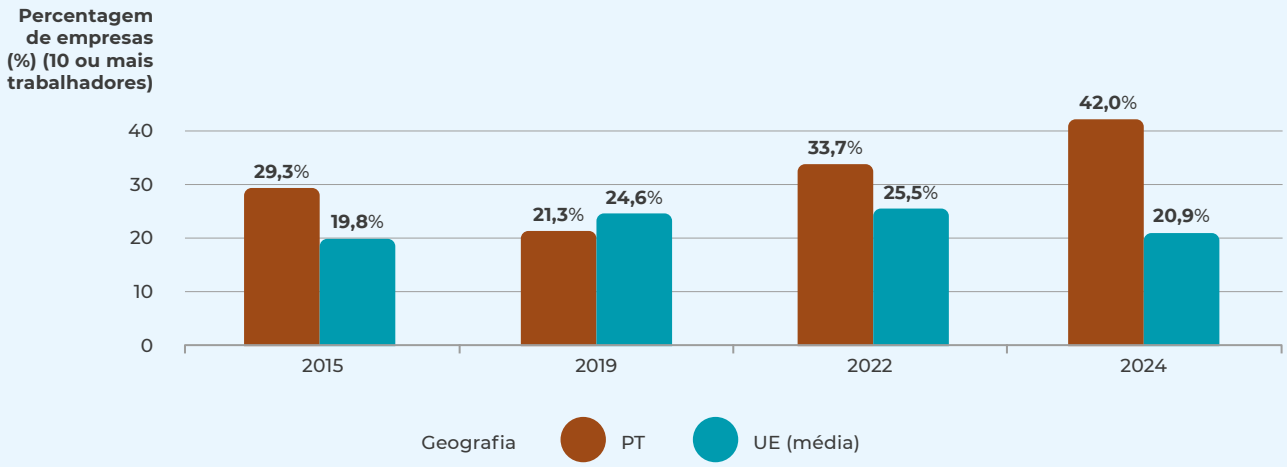
Apesar de Portugal ter apresentado, em 2019, uma percentagem de empresas a documentar medidas, práticas e procedimentos de segurança das TIC inferior à da média da UE, é de notar que a evolução foi muito significativa em 2022, com um aumento 26,1 pp colocando mesmo Portugal substancialmente acima da média da UE, 54,5% e 38,7%, respetivamente, tendo esta subida estabilizado em 2024. Nesse ano, Portugal tornou-se mesmo o terceiro Estado-Membro com maior percentagem de empresas que afirmam documentar medidas, práticas e procedimentos de segurança, ao lado da Finlândia e da Dinamarca.

Uma das razões que pode ajudar a explicar o aumento em Portugal de 2019 para 2022, é o facto de ter entrado em vigor, em 2021, a legislação nacional que regulamentou os requisitos de segurança para os operadores de serviços essenciais[5], tal como previsto na Lei n.º 46/2018, de 13 de agosto. Uma etapa importante no cumprimento dessas obrigações por parte das empresas reguladas passou pela elaboração de vários tipos de documentos, incluindo inventários de ativos, planos de segurança e relatórios anuais.

5 Decreto-Lei n.º 65/2021, de 30 de julho, que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019 (revogado).

Figura 23

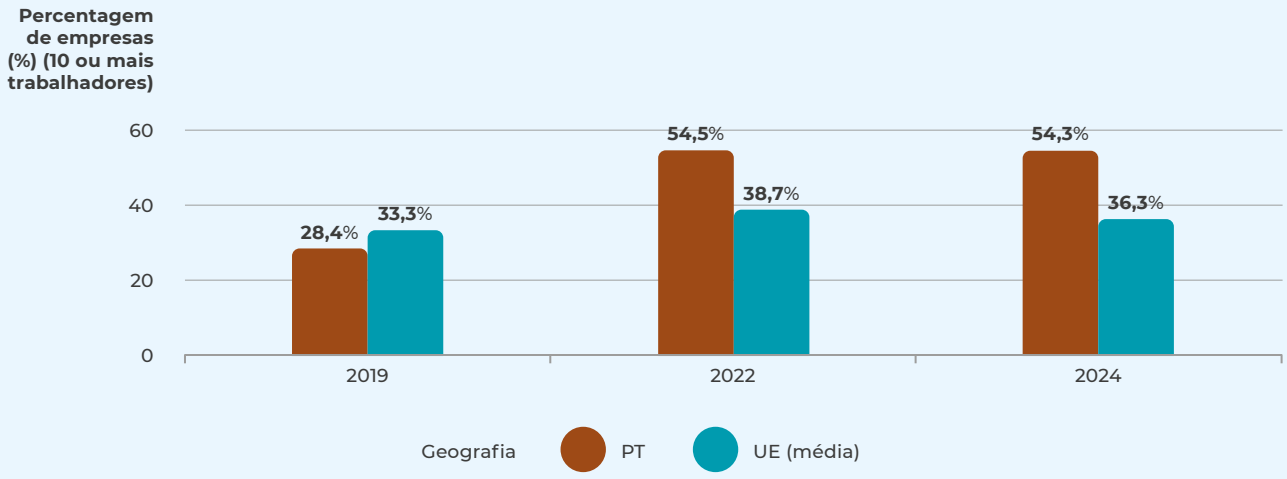
PERCENTAGEM DE EMPRESAS COM POLÍTICA DE SEGURANÇA DAS TIC DEFINIDA E REVISTA PELO MENOS NOS ÚLTIMOS 24 MESES



Fonte: Eurostat

Figura 24

PERCENTAGEM DE EMPRESAS A DOCUMENTAR MEDIDAS, PRÁTICAS OU PROCEDIMENTOS

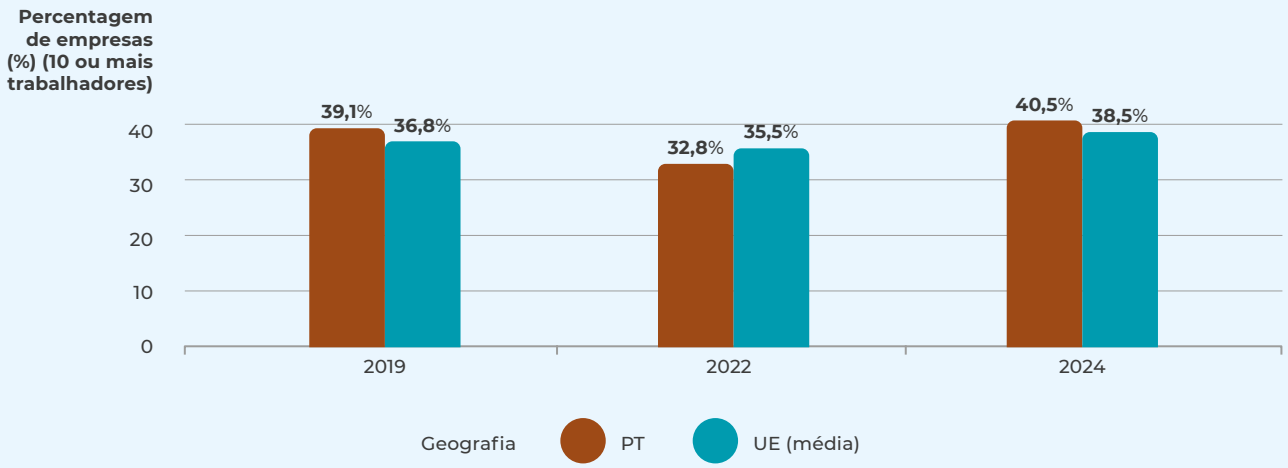


Fonte: Eurostat

Em relação à adoção de técnicas de criptografia para cifrar dados, documentos ou emails, a trajetória portuguesa revela-se mais volátil. Enquanto em 2019, a percentagem era de 39,1% em Portugal, 2,3 pp acima da média da UE, este valor baixa para 32,8% em 2022, 2,7 pp abaixo da média da UE nesse ano (35,5%). Em 2024, a média nacional volta a ser superior à da UE, em 2 pp, com 40,5% das empresas portuguesas com mais de 10 trabalhadores a afirmarem ter adotado técnicas de criptografia.

Figura 25

PERCENTAGEM DE EMPRESAS QUE IMPLEMENTARAM TÉCNICAS CRIPTOGRÁFICAS PARA CIFRAR DADOS, DOCUMENTOS OU EMAILS

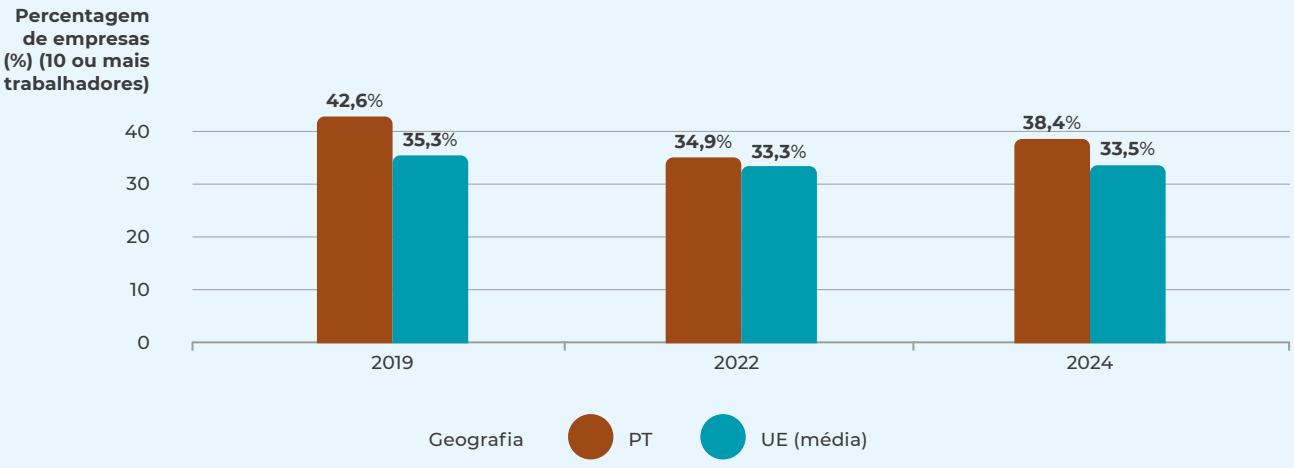


Fonte: Eurostat

Também volátil se tem mostrado a percentagem de empresas, em Portugal, a realizarem testes de segurança. Note-se, que, na definição do inquérito do Eurostat, estes testes incluem não só os testes de intrusão (*penetration test* ou *pentest*), como também testes aos sistemas de alerta e de backup e revisões às medidas de segurança. Em 2019, esta percentagem era 42,6%, um valor significativamente acima da média da UE. Contudo, verifica-se uma quebra em 2022, tanto ao nível nacional como da UE, que foi recuperada em 2024, onde a percentagem em Portugal volta a subir para aproximadamente 38%, mantendo-se 4,9 pp acima da média da UE.

Figura 26

PERCENTAGEM DE EMPRESAS A REALIZAR TESTES DE SEGURANÇA



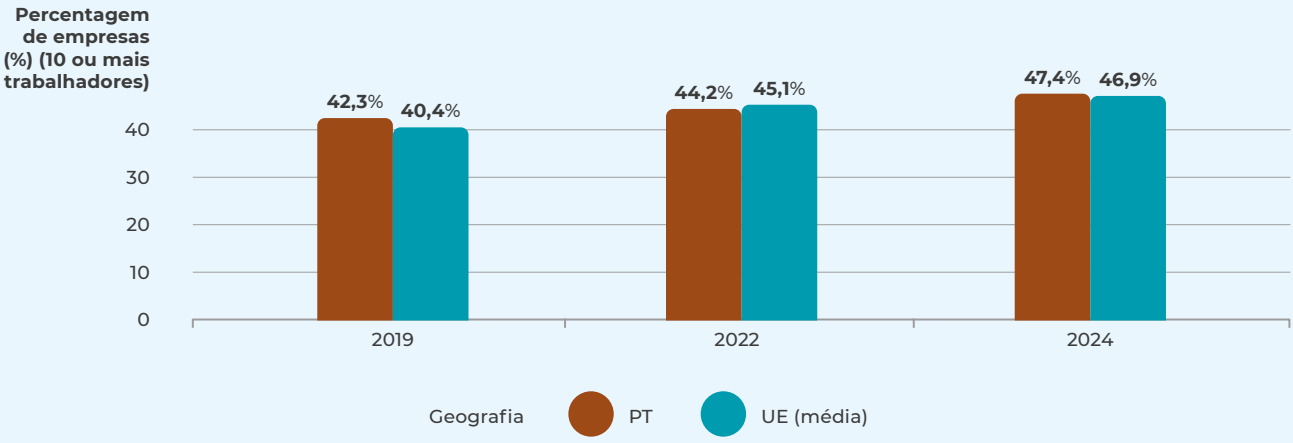
Fonte: Eurostat

Esta tendência, tanto ao nível da evolução em "U" como no facto de Portugal estar acima da média da UE desde pelo menos 2019, é também observada na implementação de gestão dos riscos de segurança das TIC. Em 2024, cerca de 37% das empresas portuguesas com mais de 10 trabalhadores afirmava implementar medidas de avaliação e gestão do risco da segurança das TIC, um valor aproximadamente 2 pp acima da média da UE.

A percentagem de empresas em Portugal a utilizar VPNs está alinhada com a média da UE, tendência que se manteve relativamente estável desde 2019, tendo vindo a subir de 42%, em 2019, para 47%, em 2024.

Figura 27

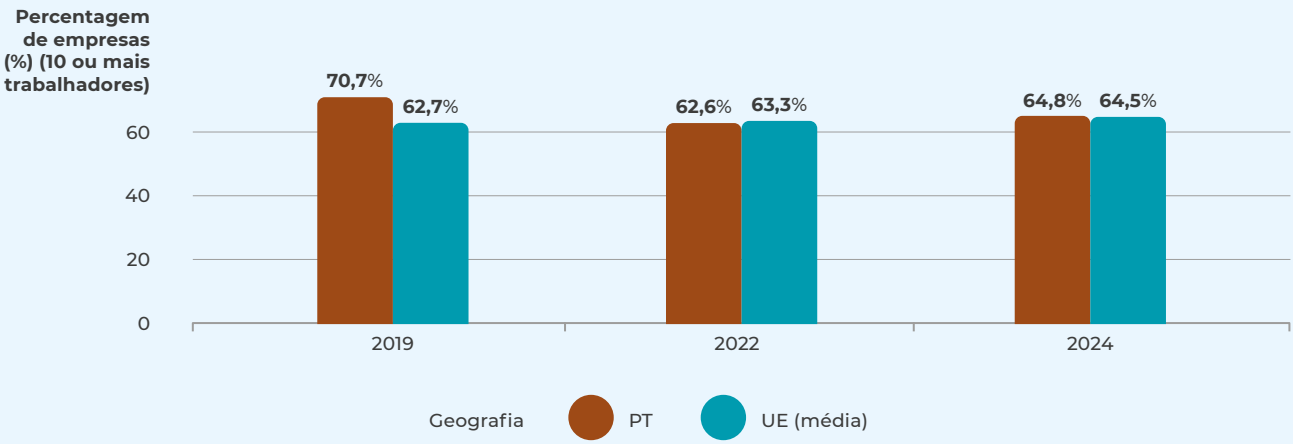
PERCENTAGEM DE EMPRESAS A UTILIZAR VPN



Fonte: Eurostat

Figura 28

PERCENTAGEM DE EMPRESAS QUE IMPLEMENTARAM CONTROLO DE ACESSOS DOS UTILIZADORES E DISPOSITIVOS À REDE DA EMPRESA (NETWORK ACCESS CONTROL)



Fonte: Eurostat

À data de 2019, a percentagem de empresas em Portugal, com 10 ou mais trabalhadores, que afirmam implementar controlos de acesso à rede estava 8 pp acima da média da UE com valores quase a atingir 71%. Contudo, deu-se uma quebra em 2022, tendo o valor descido para 62,6%, subindo apenas 2,2 pp em 2024, estando agora, e desde 2022, alinhada com a média da UE.

De acordo com os dados deste inquérito do Eurostat, Portugal tem também mantido o alinhamento com a média da UE em relação à percentagem de empresas, 75%, que afirmam adotar a prática de guardar cópias de segurança em diferentes locais, incluindo hospedados em serviços de nuvem. Estes valores têm-se mantido relativamente estáveis, tanto para Portugal como para a média da UE, desde 2019, pelo que se deduz que esta é uma das medidas de cibersegurança mais bem estabelecidas. Apenas a adoção a autenticação através de uma palavra-passe segura apresenta valores desta natureza: em Portugal, desde 2019, que 85% das empresas afirmam adotar esta medida, tendo mesmo atingido os 89% em 2024, 7,5 pp acima da média da UE.

Na implementação de várias medidas de segurança das TIC, as empresas portuguesas apresentam, em 2024, valores acima a média da UE, nomeadamente na utilização de técnicas de criptografia, na realização testes de segurança, na documentação de medidas, práticas e procedimentos de segurança das TIC e na utilização de palavras-passe fortes.

As empresas portuguesas parecem estar abaixo da média da UE, contudo, no recurso ao múltiplo fator de autenticação. Quando questionados relativamente à implementação de pelos menos dois fatores de autenticação, apenas 28% das empresas portuguesas, em 2022, responderam positivamente, sendo este um valor 4 pp abaixo da média da UE. Em 2024, esta percentagem aumenta significativamente, para 36%, mas mantem-se, contudo, ainda aquém da média da UE de 40%. A título de exemplo, do ponto de vista comparativo com outros Estados-Membros, em 2024, mais de 79% das empresas na Finlândia implementavam pelo menos dois fatores de autenticação.

Quando analisamos a implementação de métodos de autenticação biométricos, pese embora estar acima da média europeia em 2019, observaram-se aumentos significativos na implementação destas medidas por parte das empresas noutros Estados-Membros que não foram acompanhadas na mesma medida em Portugal. Em 2024, apenas 16% das empresas portuguesas implementavam esta medida face a uma média de 18% na UE. A baixa adoção destes métodos e tecnologias de autenticação em Portugal deve ser considerada particularmente preocupante tendo em conta a tendência relativa à ameaça dos *infostealers* que procuram recolher nos dispositivos eletrónicos, entre outros dados sensíveis, as credenciais de acesso a contas pessoais ou profissionais.

Estes dados são também preocupantes em relação à ameaça do *ransomware* que tem, não raras vezes, como vetor inicial de ataque o comprometimento de contas, conduzindo os atacantes a obter privilégios de acesso de administrador e a instalar o código malicioso no sistema das vítimas. A utilização do múltiplo fator de autenticação permite que um eventual comprometimento de uma palavra-passe não conduza necessariamente ao comprometimento da conta. Apesar de terem diminuído os incidentes de *ransomware* registados em 2024, estes tiveram um impacto muito significativo, nomeadamente na administração pública, que passamos a analisar.

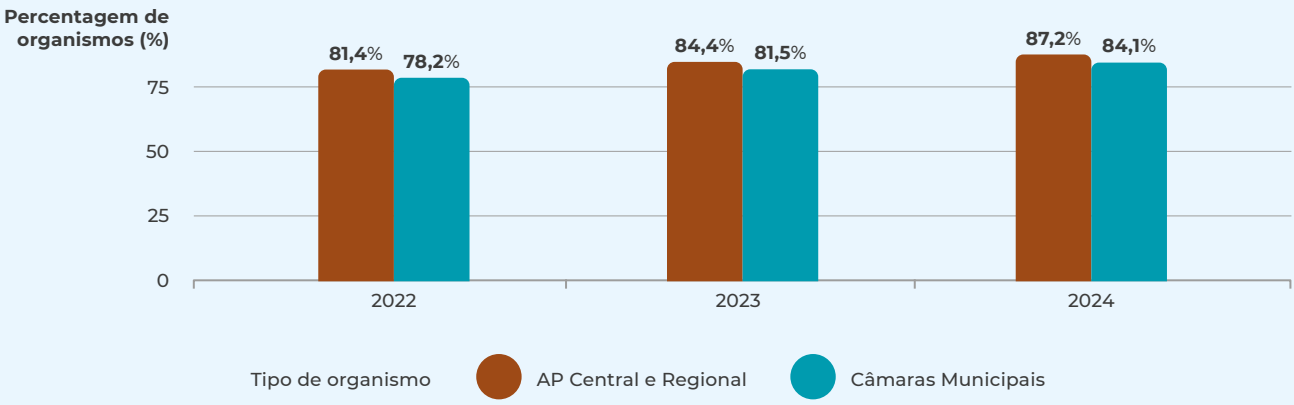
MEDIDAS DE CIBERSEGURANÇA DA ADMINISTRAÇÃO PÚBLICA

Para analisar a adoção de medidas de gestão dos riscos de segurança nas redes e sistemas de informação, e implementação de tecnologias relevantes para a cibersegurança, nos organismos da administração pública, recorremos aos dados da DGEEC (DGEEC, 2024a).

Começando com a implementação de autenticação através de palavra-passe segura, verifica-se que os valores são bastante altos, ainda que inferiores aos observados nas empresas em Portugal (cerca de 89% em 2024). Ainda assim, desde 2022, têm-se observado ligeiros aumentos em todos os tipos de organismos da administração pública na implementação deste tipo de autenticação. Os organismos da administração pública central/regional inquiridos afirmam adotar estra prática, 87%, com mais frequência que as câmaras municipais, ainda que as diferenças não sejam substanciais.

Figura 29

PERCENTAGEM DE ORGANISMOS DA AP QUE IMPLEMENTARAM AUTENTICAÇÃO ATRAVÉS DE UMA PALAVRA-PASSE SEGURA

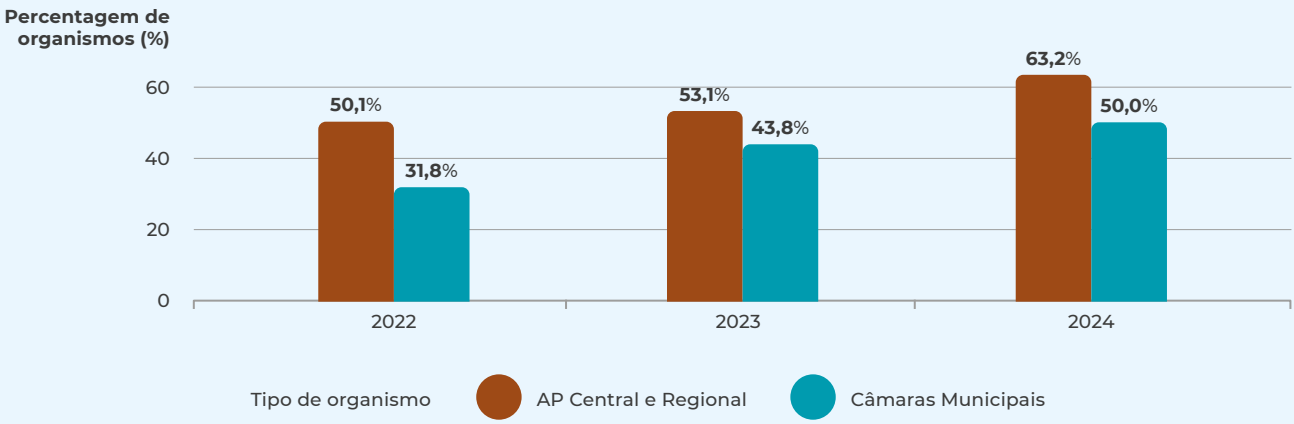


Fonte: DGEEC

Em 2024, cerca de 63% dos organismos da administração pública central/regional e metade das câmaras municipais afirmam recorrer a mecanismos de autenticação com pelo menos dois fatores. Embora estes valores não tenham ainda atingido um nível ideal, esta percentagens representam um crescimento significativo na administração pública, em relação ao ano anterior, e são substancialmente superiores àquelas observadas nas empresas com 10 ou mais trabalhadores em Portugal (36%) e na média da UE para esse segmento (40%).

Figura 30

PERCENTAGEM DE ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA A RECORRER A MÉTODOS DE AUTENTICAÇÃO COM PELO MENOS DOIS FATORES



Fonte: DGEEC

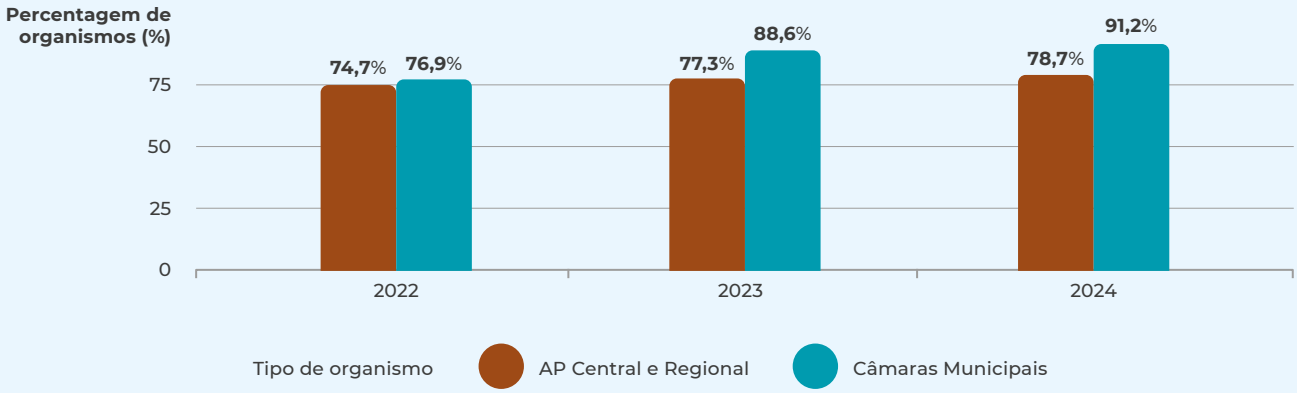
Ainda no tópico dos mecanismos de autenticação, encontramos um retrato bastante diferente no caso do recurso a mecanismos biométricos. De acordo com os dados da DGEEC, cerca de 44% das câmaras municipais e 37% da administração pública central/regional afirmaram, à data de 2024, utilizar esta família de técnicas de autenticação. Apesar da adesão ser particularmente significativa no caso das câmaras municipais, o recurso a métodos biométricos de autenticação aumentou de forma significativa em toda administração pública, com, respetivamente, aumentos de 6 e 9 pp na administração pública central/regional e nas câmaras municipais. Cumpre destacar ainda que, em todos os períodos observados, a adesão a este mecanismo é bastante maior em entidades públicas do que em entidades privadas, representado estas últimas apenas uma adesão de 16% em Portugal e de 18% na média da UE, como vimos, à data de 2024.

No que toca à adoção de técnicas de criptografia para a cifrar dados, documentos ou emails, o cenário na administração pública reverte-se, sendo possível observar uma maior implementação destas técnicas, ao longo de todo o período observado, por parte da administração pública central/regional. Em 2024, por exemplo, 59% dos organismos da administração pública central/regional afirmam recorrer a estas técnicas, face a 50% das câmaras municipais.

A manutenção de um inventário de ativos essenciais atualizado é uma condição necessária para a gestão do risco de cibersegurança. Esta medida é particularmente importante para garantir a correção atempada de vulnerabilidades nos equipamentos físicos e lógicos diminuindo, assim, a superfície de ataque suscetível de ser explorada por atores maliciosos. De acordo com os dados da DGEEC, em 2019, as percentagens de organismos da administração pública central/regional e câmaras municipais com inventário de ativos essenciais rondava, respetivamente, 75% e 77%. Estes valores têm vindo a aumentar ligeiramente na administração pública central/regional, 4 pp desde 2022. Mas é nas câmaras municipais que esta percentagem teve o aumento mais significativo, na ordem dos 14,3 pp.

Figura 31

PERCENTAGEM DE ORGANISMOS DA AP COM INVENTÁRIO DE ATIVOS

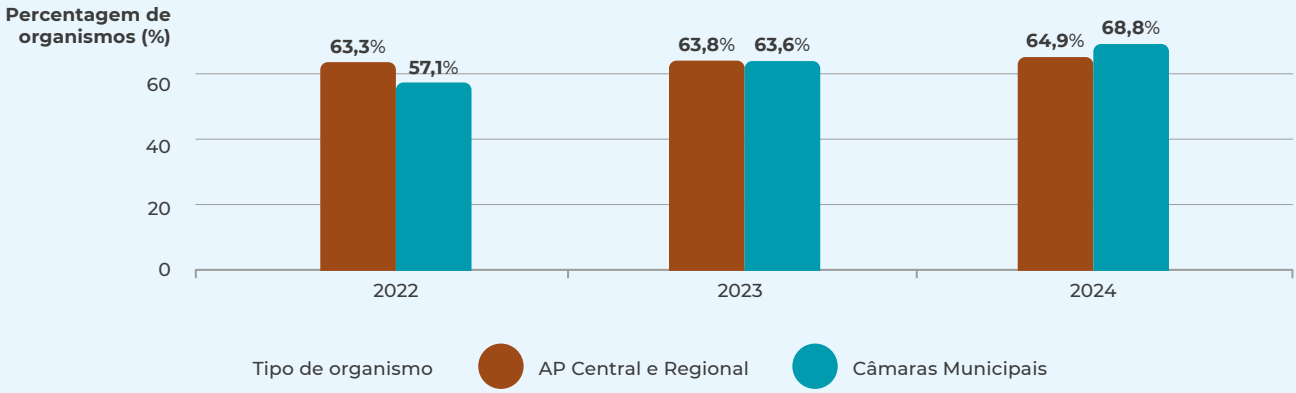


Fonte: DGEEC

Em relação à realização de análises de risco, em 2019, cerca de 63% dos organismos da administração pública central/regional e 57% das câmaras municipais inquiridas afirmaram realizar estas análises em relação aos ativos essenciais para a segurança das da TIC também. Ao longo dos anos, este cenário reverteu-se devido aos aumentos significativos na adoção desta medida por parte das câmaras municipais, na ordem dos 11,7 pp. entre 2022 e 2024, que não foram acompanhados pelos organismos da administração pública central/regional, tendo ocorrido apenas um aumento de 1,6 pp.

Figura 32

PERCENTAGEM DE ORGANISMOS DA AP A REALIZAR ANÁLISES DOS RISCOS EM RELAÇÃO A TODOS OS ATIVOS ESSENCIAIS PARA A SEGURANÇA DAS TIC



Fonte: DGEEC

Estes valores relativos à realização de inventários de ativos e respetiva análise de risco são bastante elevados na administração pública. Neste contexto, é importante recordar que o Regime Jurídico da Segurança do Ciberespaço prevê, pelo menos desde 2021, que os organismos da administração pública abrangidos por esta legislação implementem precisamente estas duas medidas[6].

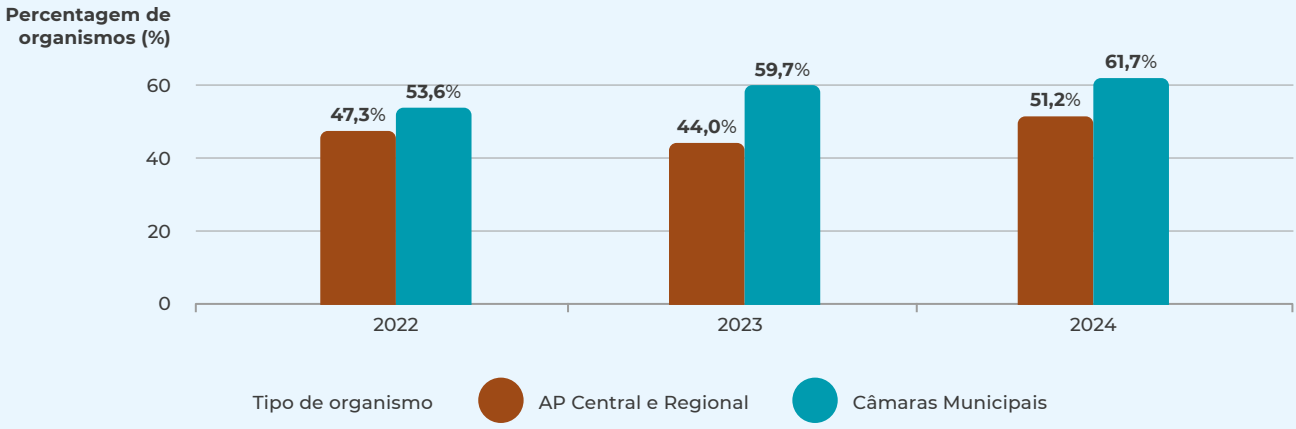
Os organismos da administração pública parecem recorrer com bastante frequência a testes de segurança das TIC. Note-se, contudo, que, na definição do inquérito da DGEEC, tal como no do Eurostat, estes testes incluem não só os testes de intrusão, como também testes aos sistemas de alerta e de *backup* e revisões às medidas de segurança. Em 2024, cerca de 63% órgãos da administração pública central/regional e 67% das câmaras municipais afirmam que recorreram a esta medida de segurança, quando a percentagem é apenas de 38% nas empresas com 10 ou mais trabalhadores em Portugal e a média da UE neste segmento de empresas se situa nos 34%. De acordo com estes dados da DGEEC, os níveis de implementação de testes de segurança nos organismos da administração pública aproximam-se da média da UE no segmento de empresas com mais de 250 trabalhadores, 71%.

Nos seus inquéritos, a DGEEC avalia também adoção da prática da manutenção de cópias de segurança em lugares externos e seguros, seguindo a chamada regra 3-2-1, isto é, três cópias dos dados, duas em formatos diferentes e pelo menos uma em local externo seguro. Os organismos da administração pública central/regional parecem realizar cópias de segurança dos seus dados seguindo esta regra numa percentagem inferior às câmaras municipais desde, pelo menos, 2022, atingindo, em 2024, o valor de 51% face aos 62% nos organismos municipais.

6 Sem que tal fosse expressamente exigido pela legislação europeia da altura, o Regime jurídico da segurança do ciberespaço (Lei n.º 46/2018, de 13 de agosto) incluiu no seu âmbito de aplicação as entidades da administração pública aquando da transposição da Diretiva (UE) 2016/1148. Como para os restantes operadores de serviços essenciais, o Decreto-Lei n.º 65/2021, de 30 de julho, exigiu aos diferentes organismos públicos o cumprimento de várias obrigações, incluindo a elaboração de um inventário de ativos (art. 6.º) e a realização de uma análise de riscos (art. 10.º).

Figura 33

PERCENTAGEM DE ORGANISMOS DA AP COM BACKUPS SEGUNDO A REGRA 3-2-1

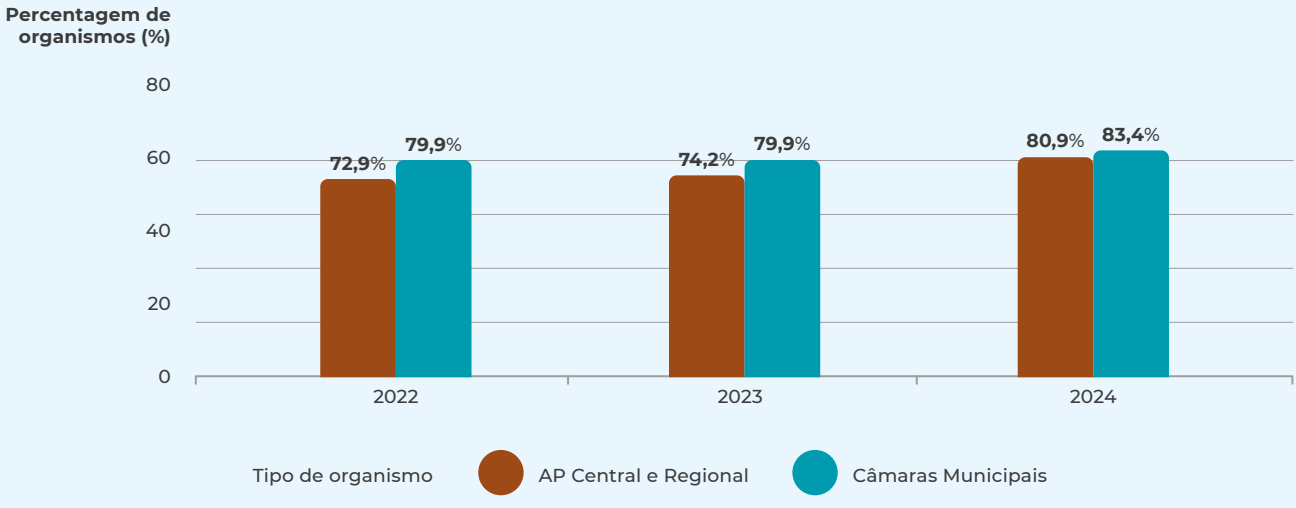


Fonte: DGEEC

Quando questionados acerca da manutenção de uma cópia de segurança em localização externa, uma medida menos onerosa do que a descrita acima, as percentagens sobem nos dois grupos, ainda que se verifique a mesma tendência ao longo do tempo. Em 2024, 81% dos organismos da administração pública central/regional tinha cópias de segurança de informação numa localização externa, enquanto 83% dos organismos municipais adotaram esta prática.

Figura 34

PERCENTAGEM DE ORGANISMOS DA AP QUE FIZERAM CÓPIAS DE SEGURANÇA DE INFORMAÇÃO EM LOCALIZAÇÃO EXTERNA



Fonte: DGEEC

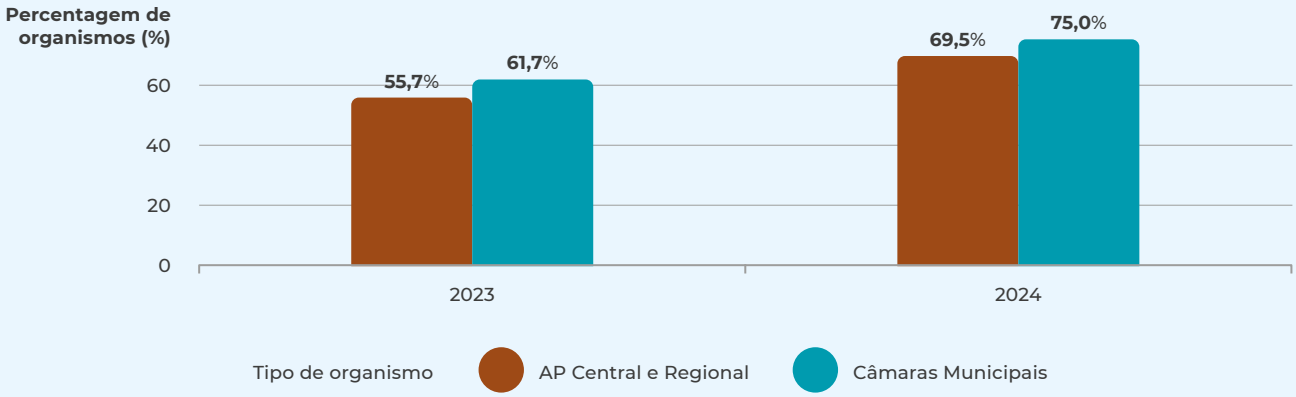
Ainda no tópico das cópias de segurança, os inquéritos da DGEEC avaliam também a percentagem de organismos da administração pública a implementar cópias de segurança imutáveis (‘*Write Once, Read Many*’ ou *WORM*), particularmente relevantes enquanto primeiras linhas de defesa contra ataques de *ransomware*, pois como os dados não podem ser modificados, também não podem ser cifrados, tornando o *malware* ineficaz. Enquanto em 2023, a percentagem rondava os 38% tanto na administração pública central/regional e nas câmaras municipais, este valor subiu para 45%, no caso da primeira, e para 50%, no caso da última em 2024.

Embora seja difícil analisar este aumento de forma causal, a evolução da perceção sobre esta ameaça, em Portugal, pode ter contribuído para este aumento. Desde que o CNCS começou a realizar o inquérito *Perceção de risco no ciberespaço de interesse nacional* junto das comunidades de cibersegurança, que o *ransomware* tem figurado no pódio das ciberameaças mais relevantes, com a administração pública local a ser um alvo particularmente afetado. Entre 2020 e 2022, a percentagem de inquiridos que considerava o *ransomware* como uma ameaça relevante passou de 65% para 89% (CNCS, 2023, p. 73). Em 2023, verifica-se uma descida para 58%, mas a percentagem volta a subir para os valores próximos dos anteriores em 2024, 69% (CNCS, 2025, p. 68-69).

Olhando para os dados relativos à adoção de tecnologias cruciais para combater as diferentes ciberameaças descritas acima, vemos uma adesão quase total, em 2024, ao *software* antivírus (99% na administração pública central/regional e 100% nas câmaras municipais), à *firewall* (98% e 99%), aos filtros anti-*spam* (97% em ambos os tipos de organismo público) e à segurança de correio eletrónico (96% também em ambos). Observamos, contudo, uma adesão mais moderada, ainda que substancial, relativamente aos sistemas de gestão de *endpoints* que permitem a monitorização, gestão e proteção dos dispositivos eletrónicos conectados às redes dos organismos. Em 2024, 70% dos organismos da administração pública central/regional e 75% câmaras municipais recorreram as estas tecnologias, um aumento de 13,8 pp e 13,3 pp, respetivamente, em relação a 2023.

Figura 35

PERCENTAGENS DE ORGANISMOS DA AP A UTILIZAR TECNOLOGIAS DE GESTÃO DE ENDPOINT



Fonte: DGEEC

A evolução na implementação de medidas de cibersegurança da administração pública está correlacionada com o nível de ameaça para este setor. Acima observamos que, em 2024, verificou-se um aumento acentuado no número de incidentes registados na administração pública, nomeadamente a administração local (26%) e regional (74%). As medidas acima analisadas não permitem fazer face a algumas ameaças consideradas relevantes e transversais a todos os setores, como é o caso dos *infostealers* e do DDoS (CNCS, 2025, p. 10). Assim, e apesar do elevado grau implementação de algumas destas medidas, o número de incidentes e impacto destes na administração pública mostra que pode não ser suficiente.

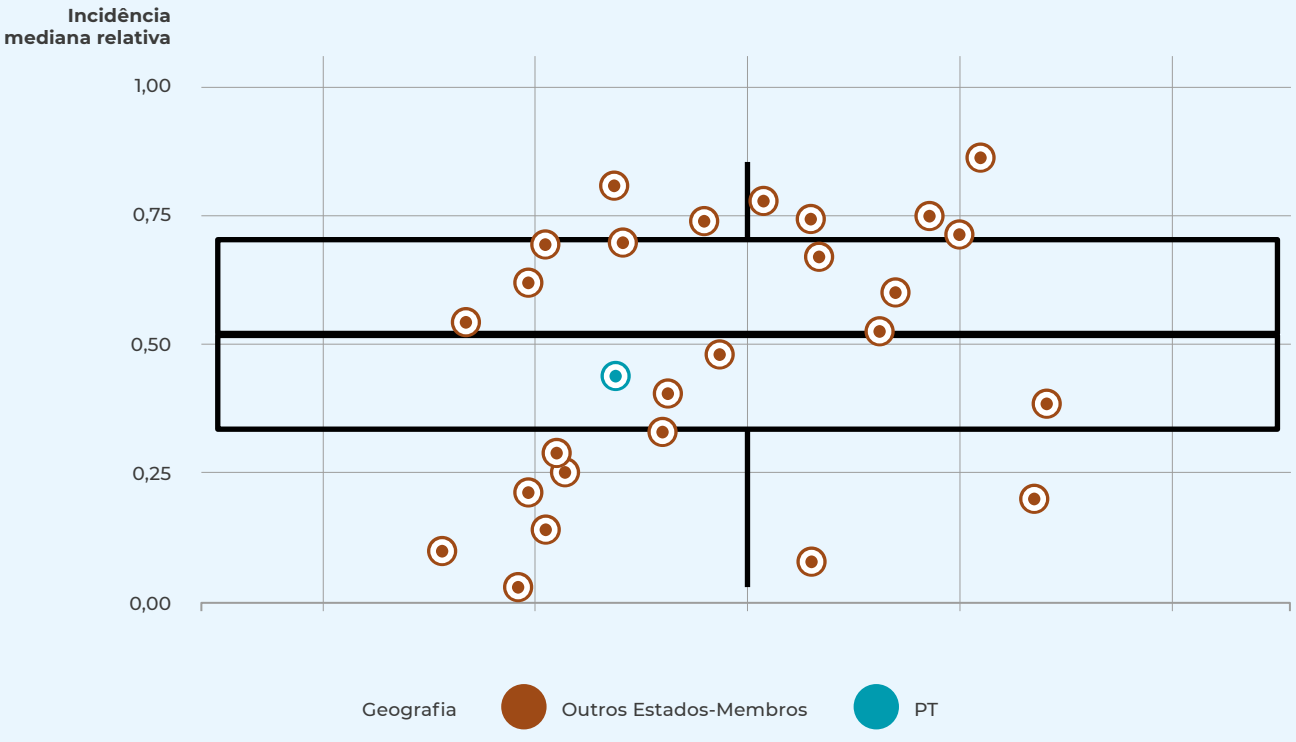
VULNERABILIDADES TÉCNICAS E COMUNICAÇÕES SEGURAS

EXPLORAÇÃO DE VULNERABILIDADES TÉCNICAS

O aumento da exploração de vulnerabilidades para fins maliciosos foi uma das tendências observadas no Relatório ReC de 2025. O número de notificações do tipo sistema vulnerável recebidas pelo CERT.PT, à data de novembro de 2025, aumentou 279% desde 2021, representando 29% do total de notificações recebidas da classe de vulnerabilidade, segundo a taxonomia da Rede Nacional de CSIRT (RNCSIRT). Em 2025, a ENISA voltou a referir que a exploração de vulnerabilidades continua a ser o vetor de intrusão mais prevalente, logo depois do *phishing*, sendo que na grande maioria dos casos a exploração da vulnerabilidade culmina numa intrusão do sistema, seguido da distribuição de *malware* (ENISA, 2025, p. 8). Estas tendências sugerem que uma análise da superfície de ataque da sociedade portuguesa não pode ignorar uma análise do panorama nacional de sistemas vulneráveis.

Figura 36

DISTRIBUIÇÃO DE VALORES DE INCIDÊNCIA MEDIANA RELATIVA DE VULNERABILIDADES NOS 27 ESTADOS-MEMBROS



Fonte: Shadowserver/CNCS

Para analisar a incidência relativa de vulnerabilidades recorreu-se aos dados de fonte aberta da Fundação *Shadowserver*[7]. Esta organização sem fins lucrativos recolhe, através de vários métodos telemétricos e varrimentos na internet, dados relativos à incidência de variantes de código malicioso, *bots*, vulnerabilidades técnicas, serviços indevidamente expostos à internet, entre outros. Para esta análise, começou-se por recolher informação relativa à incidência de 148 vulnerabilidades, em Portugal e noutros países, relativamente a 2024. Mais concretamente, para cada uma das vulnerabilidades recolheu-se o número de endereços de IPs reportados normalizado por milhão de população (ou *per capita*). Com base nos identificadores dos CVEs, enriquecemos os dados com contexto sobre a vulnerabilidade com recurso aos dados da base de dados *Known Exploited Vulnerabilities* (KEV) da *Cybersecurity and Infrastructure Security Agency* dos Estados Unidos da América (CISA). A métrica utilizada[8], que denominámos de incidência mediana relativa tem por benefício normalizar dados relativamente a países com dimensões substancialmente diferentes, deve ser interpretada da seguinte forma:

- Valores próximos de 1: indicam países com mais vulnerabilidades *per capita* (ocupando posições mais elevadas no *ranking*);
- Valores próximos de 0: indicam países com menos vulnerabilidades *per capita* (ocupando posições mais baixas no *ranking*).

Na figura 36 temos um diagrama do tipo *box-plot*, que nos permite visualizar a mediana, a linha que separa cada metade da "caixa", e os quartis. Os pontos nesta visualização são os resultados deste indicador para cada um dos Estados-membros. Estão todos anonimizados menos Portugal, representado a azul. Como é possível observar, o indicador de incidência mediana relativa com o valor de 0,44 coloca Portugal relativamente perto da mediana da distribuição de valores deste indicador. Este resultado é expectável tendo em conta que Portugal se encontra no 12º lugar no *ranking* dos 27 Estados-membros com um maior valor mediano de endereços de IPs vulneráveis *per capita*.

À luz desta análise, e apesar das tendências observadas em relação ao aumento da exploração de vulnerabilidades no ciberespaço, Portugal não se destaca como um país excessivamente exposto à exploração de vulnerabilidades técnicas. No entanto, deve ser tido em conta, por um lado, a existência de vulnerabilidades desconhecidas ou recentemente identificadas, mas para as quais ainda não existe uma correção disponível (*zero-days*); por outro lado, fica evidente a existência de um grande número de vulnerabilidades, *per capita* em Portugal, que não foram corrigidas apesar de terem sido identificadas e corrigidas pelo fabricante há vários anos. Como constatado anteriormente, verificou-se que muitas das vulnerabilidades associadas a incidentes em 2024 podiam ter sido mitigadas, em particular, tendo em conta a existência de medidas de mitigação disponíveis desde há vários anos[9].

Nem todas as vulnerabilidades apresentam o mesmo grau de severidade, nem todos os ciberataques têm o mesmo impacto. O gráfico abaixo mostra a distribuição dos números de endereços de IP nacionais vulneráveis por milhão de habitantes[10] relativamente às vulnerabilidades com maior incidência em Portugal. Segmentamos, nesta análise, se a vulnerabilidade é conhecida por já ter sido utilizada no contexto de campanhas de *ransomware*, utilizando, para o efeito, a base de dados KEV da CISA[11]. Por exemplo, a vulnerabilidade CVE-2024-21762[12], uma das mais relevantes segundo dados analisados, já terá sido utilizada em ataques de *ransomware*[13].

7 https://www.shadowserver.org/

8 Ver metodologia utilizada para elaborar esta métrica no anexo.

9 CNCS, *Relatório Cibersegurança em Portugal – tema Riscos & Conflitos*, 6.ª ed., 2025, p. 85.

10 Na escala de log 10 devido à presença de valores extremos.

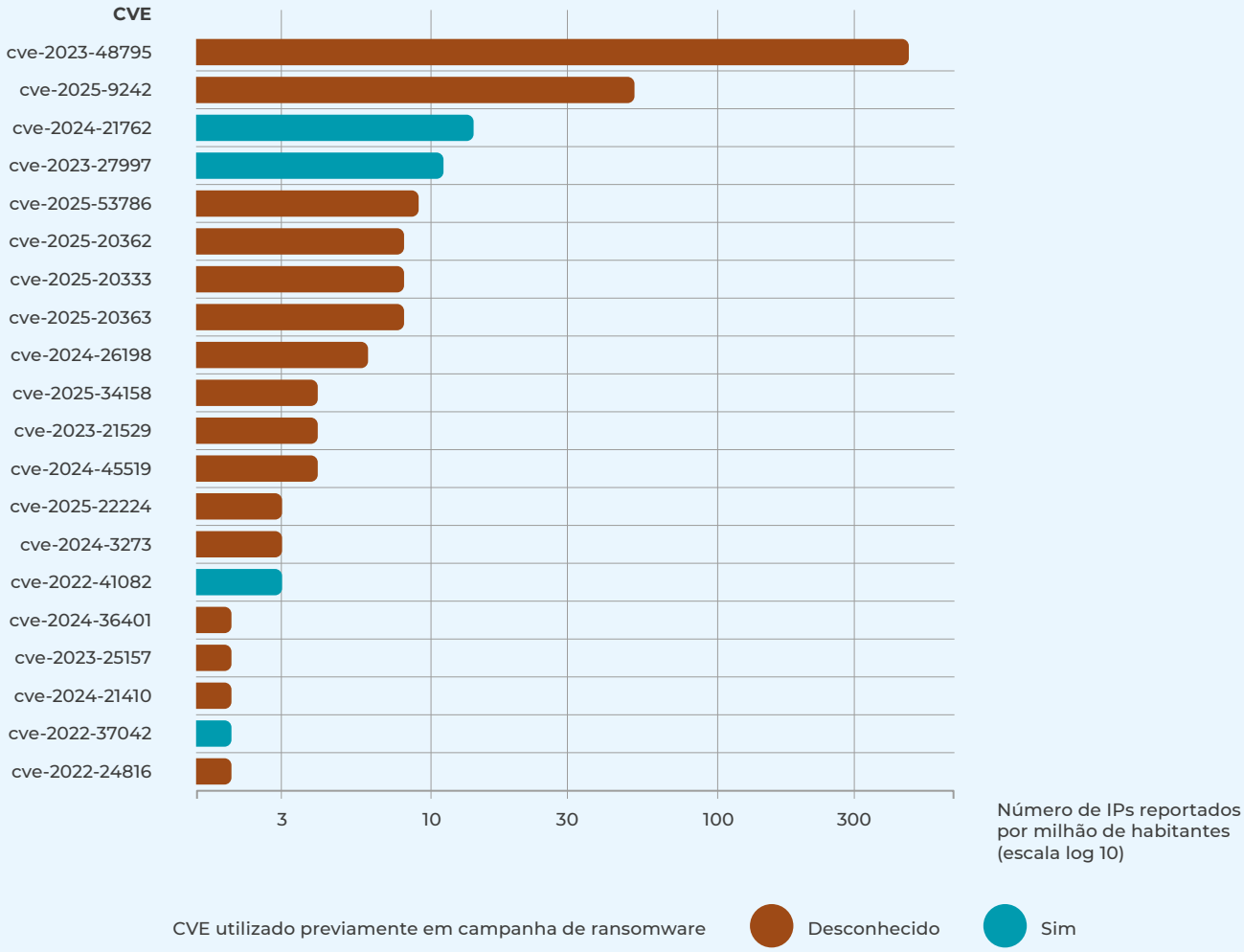
11 https://www.cisa.gov/known-exploited-vulnerabilities-catalog

12 Ver alerta de vulnerabilidade do CNCS relativo ao Fortinet FortiOS, 9 de fevereiro de 2024 (consultado 11 de fevereiro 2026) URL: https://dyn.cncs.gov.pt/pt/alerta-detalhe/art/135844/alerta-de-vulnerabilidades-fortinet-fortios

13 Gatlan, Sergiu. Critical Fortinet flaws now exploited in Qilin ransomware attacks. Bleeping Computer. https://www.bleepingcomputer.com/news/security/critical-fortinet-flaws-now-exploited-in-qilin-ransomware-attacks/

Figura 37

INCIDÊNCIA DE DETERMINADOS CVES EM PORTUGAL DURANTE 2025 NA ESCALA DE LOG 10



Fonte: Shadowserver/CNCS/CISA

NOVO QUADRO DE GESTÃO COORDENADA DE VULNERABILIDADES

A recente legislação europeia de cibersegurança veio enquadrar a gestão de vulnerabilidades técnicas exigindo a designação de uma entidade nacional coordenadora para efeitos da divulgação coordenada de vulnerabilidades, a existência de uma política nacional para esse efeito, e a possibilidade que pessoas e organizações comuniquem vulnerabilidades, de forma anónima se assim o solicitarem.

Em Portugal, o novo Regime Jurídico da Cibersegurança designou o CERT.PT, que funciona junto do CNCS, como entidade coordenadora neste âmbito, passando a agir como intermediário de confiança entre investigadores no domínio da segurança da informação e os fabricantes ou fornecedores de produtos ou prestadores de serviços TIC.

Em linha com as melhores práticas internacionais[14], este regime foi acompanhado de uma alteração à Lei do Cibercrime (Lei n.º 109/2009) que prevê um mecanismo de exclusão da punibilidade de atos ilícitos praticados por investigadores, nomeadamente os crimes de acesso ou interferência ilegítima (artigos 6.º e 7.º), desde que o investigador atue dentro dos limites legais estipulados, estando excluída a obtenção de vantagem económica assim como a utilização da engenharia social, furto de palavras-chave, instalação de *malware*, eliminação ou alteração de dados.

COMUNICAÇÕES SEGURAS

A utilização da internet comporta riscos para a segurança e privacidade dos utilizadores. Os dados dos utilizadores podem ser intercetados e recolhidos sem o seu conhecimento e consentimento devido a conexões não seguras. Durante os últimos anos, foram desenvolvidas várias normas técnicas, protocolos, políticas de segurança e encriptação que procuraram reforçar a segurança da infraestrutura da internet e tornar, por sua vez, a sua utilização mais segura. Estes *standards* não são sempre implementados por defeito e estão longe de ser obrigatórios ou gratuitos pelo que a sua adoção requer muitas vezes a ação de diferentes atores: tradicionalmente por parte dos administradores de *websites* ou servidores de *email*, mas por vezes a adoção destes *standards* tem de ocorrer ao nível de associações, operadores de infraestruturas digitais, governos ou organizações internacionais. Nesta secção é analisado o nível de adoção de alguns dos *standards* relevantes para avaliar o estado da arte das comunicações seguras no ciberespaço nacional.

Quando as comunicações não são cifradas, a integridade e confidencialidade do tráfego de internet do utilizador podem ser facilmente comprometidas. Nesse caso, a transmissão de dados entre o *browser* do utilizador e a página de internet efetua-se em texto simples, ficando exposta aos riscos de interceção, rastreamento e alteração dos mesmos. Isto é particularmente preocupante quando os dados transmitidos incluem credenciais ou outra informação sensível. Noutros casos, atacantes podem comprometer a integridade das páginas visitadas ao intercetar e adulterar as comunicações entre estas e os utilizadores, seja injetando código malicioso nos conteúdos das páginas, seja redirecionando o utilizador para sites maliciosos.

Para fazer face a estes riscos, foi desenvolvida uma versão mais segura do *Hypertext Transfer Protocol* (HTTP), protocolo que permite a comunicação entre um servidor *web* e um utilizador, que suporta a cifragem do tráfego de internet, através do protocolo SSL/TLS. A esta versão mais segura do protocolo HTTP, conhecida por *Hypertext Transfer Protocol Secure* (HTTPS), acresce a possibilidade de os servidores obrigarem os browsers a aceitarem apenas comunicações via HTTPS. Este mecanismo conhecido por HTTP *Strict Transport Security* (HSTS) é, por isso, crucial para garantir uma implementação eficaz do HTTPS.

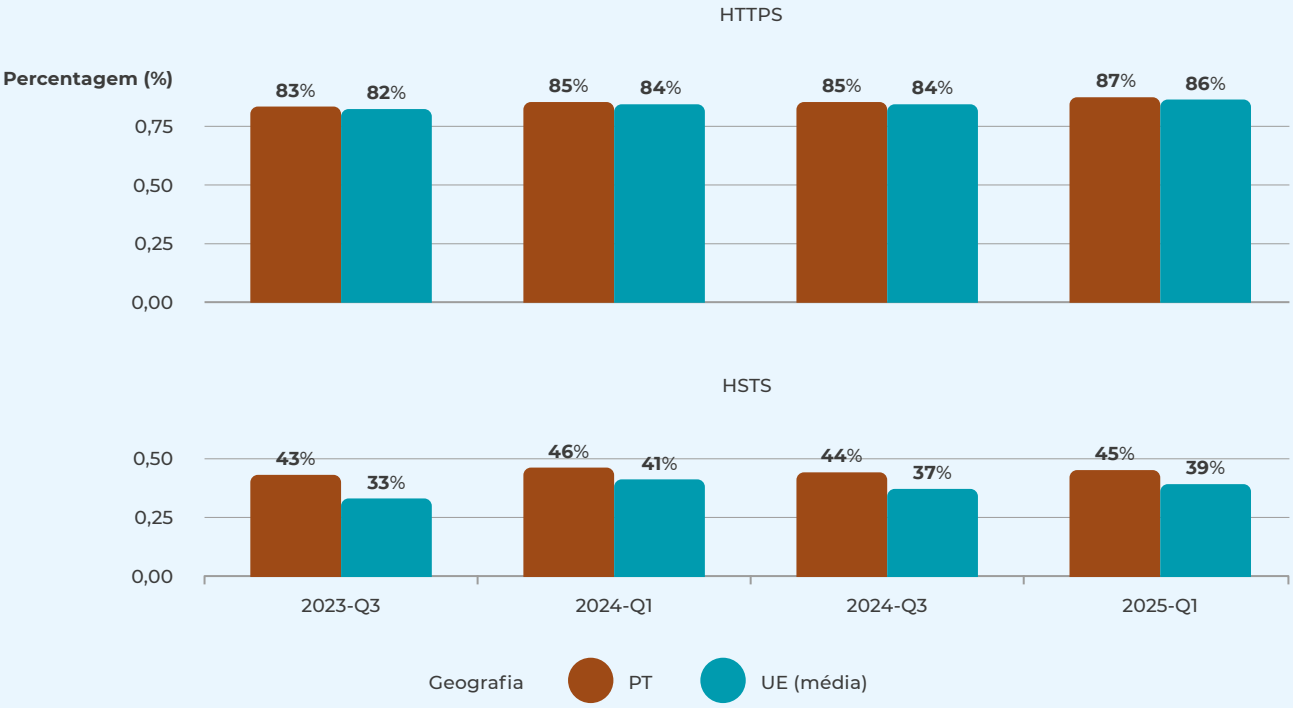
Abaixo, na figura 38, mostramos uma análise da adoção de HTTPS e HSTS com base nos dados relativos ao projeto *Key Internet Standards Deployment Monitoring* (KISDM), desenvolvido pelo *Directorate General for Communications Networks, Content and Technology* e do *Joint Research Centre* (DG CONNECT & JRC, 2025) da Comissão Europeia, que recorre a dados públicos ou a *scanners* desenhados para o efeito, para avaliar a adoção de *standards* nas páginas mais visitadas do mundo e em cada Estado-Membro[15]. Relativamente à adoção do protocolo HTTPS, Portugal parece estar, no primeiro trimestre de 2025, ligeiramente acima da média da UE com 87% das páginas analisadas face a 86% no caso da UE. Esta tendência existe pelo menos desde o terceiro trimestre de 2023. A diferença, contudo, parece ser mais marcada no que toca ao recurso a HSTS. No primeiro trimestre de 2025, observava-se uma taxa de adoção 6 pp acima da média da UE, que conta com 45%. Este diferencial existe pelo menos desde o terceiro trimestre de 2023, tendo decrescido de 10 pp no terceiro trimestre de 2023 para o valor atual.

14 OECD. (2021). Encouraging Vulnerability Treatment: Overview for policy makers, OECD Digital Economy Papers, no. 307, URL: https://www.oecd.org/en/publications/encouraging-vulnerability-treatment_0e2615ba-en.html ; NIS Cooperation Group. (2023) *Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies*, URL: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

15 Para mais detalhes sobre as fontes de dados e técnicas de instrumentação utilizadas nas mensurações, ver relatório de Kouliaridis & Kounelis (2025a).

Figura 38

PERCENTAGEM DE ADOÇÃO DE HTTPS E HSTS



Fonte: DG Connect/JRC

Antes da sua versão 1.3, as primeiras versões do protocolo TLS ficaram associadas a várias fragilidades e a criptografia fraca, tendo-se considerado que a segurança e confidencialidade das comunicações não estariam suficientemente garantidas[16]. Abaixo, utilizando dados do *Portugal Chapter da Internet Society Foundation* (ISOC-PT)[17], analisamos a percentagem de páginas auditadas, por tipo, que suportam a versão mais recente do protocolo TLS. Ao contrário dos dados do projeto KISDM, que nos mostram a proporção relativa ao equivalente da população relevante da internet, os dados do ISOC-PT analisam a implementação de *standards* relevantes para as comunicações seguras e para a cibersegurança por parte de sites sociologicamente relevantes, como páginas de internet de organismos públicos, órgãos de comunicação social ou de empresas cotadas no índice *Portuguese Stock Index* 20 (PSI 20), um *proxy* para as grandes empresas portuguesas.

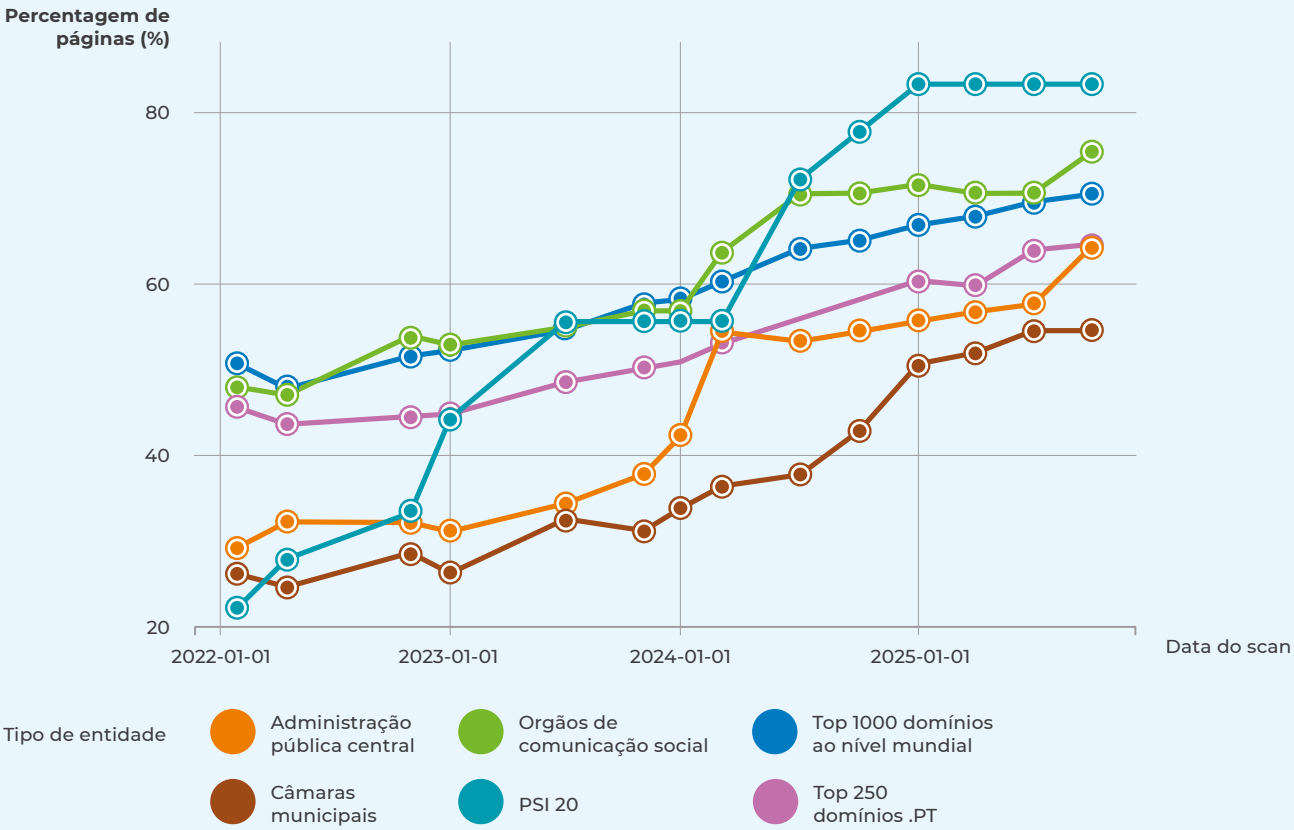
A setembro de 2025, o tipo de entidade nacional com a maior percentagem de páginas a suportar esta versão do protocolo de segurança foi o das empresas cotadas no índice PSI 20 com cerca de 83% das páginas. É de referir que se têm observado melhorias significativas recentes neste segmento, com um aumento de aproximadamente 27 pp desde fevereiro de 2024. A este grupo segue-se o das páginas dos órgãos de comunicação social (OCS), com 76% das páginas a suportarem a versão 1.3 do protocolo TLS.

É digno de nota o facto destes dois segmentos nacionais apresentarem percentagens superiores às dos 1000 domínios mais visitados a nível mundial (71%) e dos 250 domínios mais populares com o nome de domínio de topo ".PT" (64,6%). Esta última percentagem é, por sua vez, virtualmente idêntica à da administração pública central (64,4%) e encontra-se bem acima das menores percentagens que encontramos nas câmaras municipais. Em todos os segmentos é observável uma tendência de crescimento na utilização da versão mais atual do protocolo TLS ainda que se observem diferenças no ritmo das trajetórias.

16 https://www.ietf.org/rfc/rfc8446.html
17 https://observatory.isoc.pt/domains.html

Figura 39

PERCENTAGEM DE PÁGINAS A SUPORTAR TLS 1.3., POR TIPO



Fonte: ISOC-PT

O sistema de roteamento da Internet é vulnerável a várias ameaças e riscos. Enquanto os dados atravessam a internet de uma rede para outra, podem ser intercetados, bloqueados ou desviados, de forma acidental ou intencional, provocando disrupções no tráfego, violações de privacidade e danos financeiros.

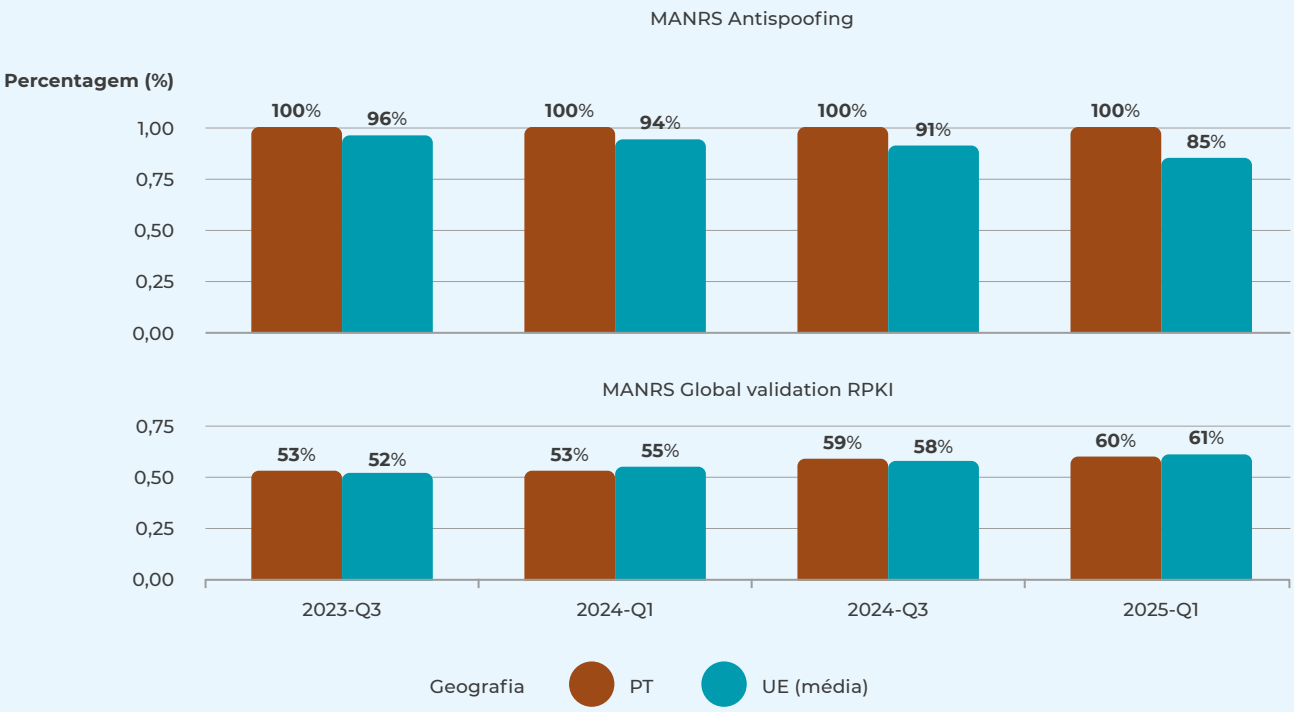
Para garantir a segurança e fiabilidade do roteamento da Internet, foram definidas normas ao nível internacional, baseadas no protocolo *Border Gateway Protocol* (BGP) aplicando-se por isso, sobretudo, a entidades que fornecem pontos de troca de tráfego, serviços de comunicações eletrónicas acessíveis ao público e redes de distribuição de conteúdos, numa iniciativa global conhecida por *Mutually Agreed Norms for Routing Security* (MANRS)[18]. Esta iniciativa prevê a adoção de várias normas e ações de natureza obrigatória e voluntária por parte destas entidades. Nestas últimas encontram-se, nomeadamente, a adoção de ações que impeçam a falsificação de endereços de IP (*antispoofing*) e que permitam a validação de informação relativa ao roteamento do tráfego de internet à escala global através da tecnologia *Resource Public Key Infrastructure* (RPKI). Precisamente por não serem obrigatórias, são analisadas de seguida a adoção destas duas ações recorrendo aos dados do projeto KISDM (EC, 2025).

Em relação à adoção de medidas *antispoofing*, a adesão parece ser total em Portugal durante todo o período observado. Note-se, contudo, que isto é também o caso para vários Estados-membros, verificando-se níveis de adesão semelhantes em 13 dos 27. Note-se, contudo, que a taxa de adoção (%) das recomendações MANRS relativas à validação de rotas através da tecnologia RPKI é substancialmente inferior. No terceiro trimestre de 2023, a taxa de adesão rondava os 53%, mais 1 pp que a média da UE. Por outro lado, observa-se também um aumento gradual e sustentado na adoção desta medida em Portugal que resultou em valores a rondar os 60%, no primeiro trimestre de 2025, ainda assim, menos 1 pp que a média da UE.

18 https://manrs.org/

Figura 40

PERCENTAGEM DE ADOÇÃO DE RECOMENDAÇÕES MANRS ANTISPOOFING E VALIDAÇÃO DE ROTA COM RPKI



Fonte: DG Connect/JRC

AMEAÇAS AO ROTEAMENTO DA INTERNET

O *Border Gateway Protocol hijacking* ocorre quando um agente malicioso se faz passar por uma rede que não lhe pertence, através do sequestro de grupos de endereços de IP que não lhe pertencem, redirecionando o tráfego da internet para um destino da sua conveniência. Este tipo de técnica é utilizado em diferentes tipos de ciberataques como, por exemplo, quando o tráfego é encaminhado para provocar a sobrecarga de um servidor ou página de internet num ataque de DDoS, para intercetar o tráfego de internet de modo a evitar o acesso dos utilizadores a determinadas páginas de internet ou para reencaminhar os utilizadores para páginas maliciosas que colonizam páginas de serviços legítimos com vista à captura de credenciais de acesso.

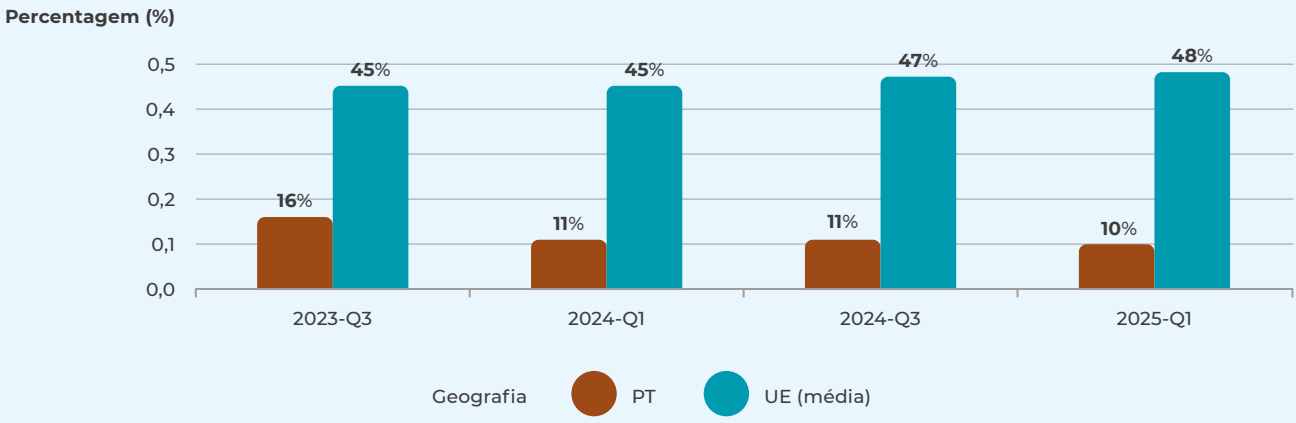
O IP *spoofing* consiste na modificação de endereços de IP que estão na origem de uma comunicação, permitindo ocultar a identidade do remetente ou fazendo-se passar por outro sistema de informação. Esta técnica é utilizada com frequência em ataques de DDoS e, quando modificado de forma aleatória, dificultar o bloqueio deste tipo de ataques assim como o processo de atribuição de ciberataques.

Para a maioria dos utilizadores, o acesso à internet começa quase sempre com um nome de domínio. Ao inserir o nome de uma página de internet no *browser* de um dispositivo eletrónico, este último traduz o nome de domínio num endereço de IP. Durante este processo, é particularmente importante garantir que o utilizador não será redirecionado para outras páginas potencialmente maliciosas sem que disso se aperceba. Imagine-se, por exemplo, um utilizador que pretende aceder à sua conta bancária e proceder a um pagamento, mas acaba por ser redirecionado para uma página ilegítima que coloniza o grafismo da página da sua instituição bancária. Para garantir a autenticidade e integridade da informação comunicada entre servidores DNS e destes com as aplicações dos utilizadores, foram criadas extensões de segurança criptográfica ao nível do protocolo DNS, conhecida em inglês por *Domain Name System Security Extensions* (DNSSEC).

Apesar da sua importância para prevenir diversos tipos de ciberataques, a adoção desta tecnologia em Portugal ainda é particularmente baixa. Com base nos dados do projeto KISDM (EC, 2025), verifica-se que a validação de respostas HTTPS com recurso a DNSSEC está 38 pp abaixo da média da UE, com uma taxa de adesão de apenas 10%, no primeiro trimestre de 2025, em Portugal. Note-se também que Portugal e a UE parecem encontrar-se numa trajetória em contraciclo. Enquanto a tendência em Portugal tem sido de uma moderada diminuição entre o terceiro trimestre de 2023 e o primeiro de 2026 (-6 pp), a da média na UE tem sido de aumento, ainda que ligeiro (3 pp).

Figura 41

PERCENTAGEM DE ADOÇÃO DE DNSSEC

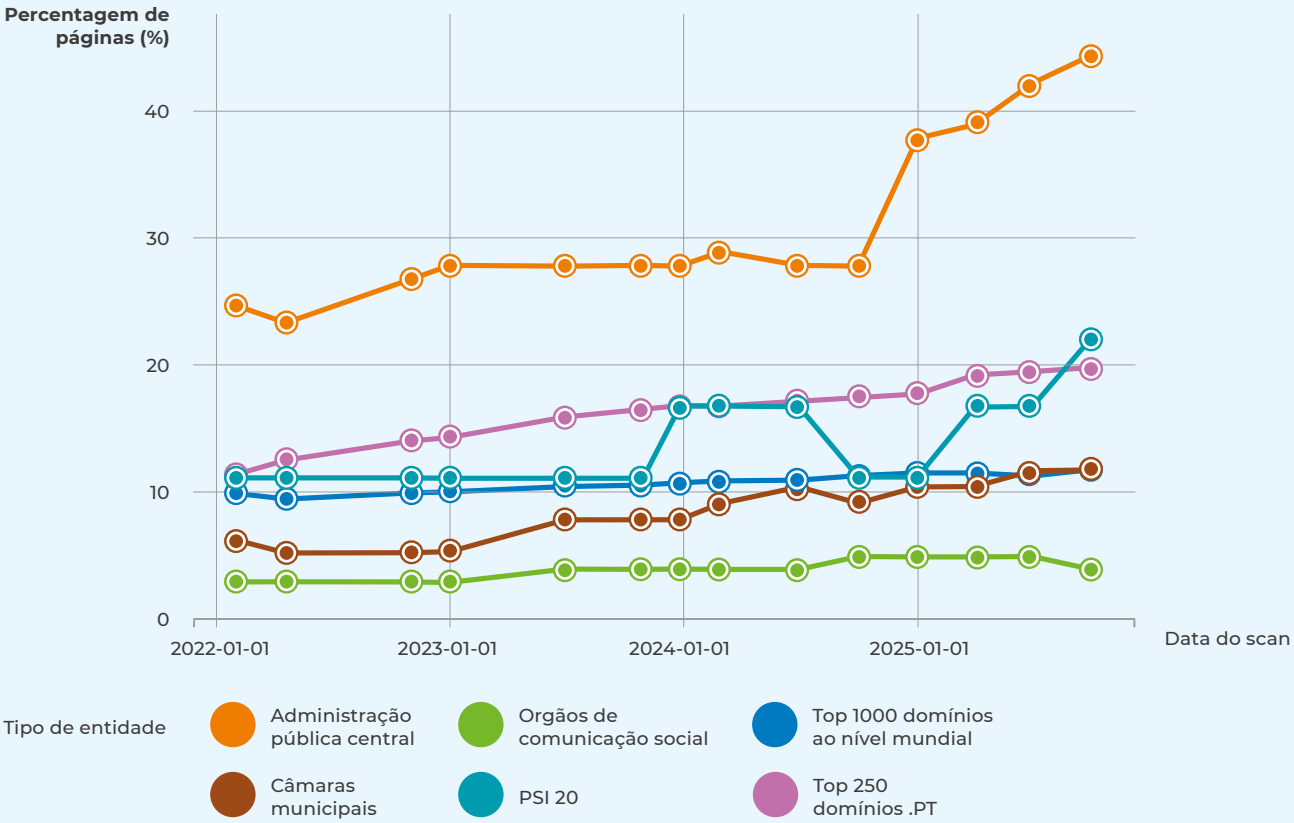


Fonte: DG Connect/JRC

Este panorama nacional relativo à adoção do DNSSEC apresenta variações importantes de acordo com o tipo de entidade que detém nomes de domínio. Com base em dados do ISOC-PT, é possível constatar que os organismos da administração pública central são, pelo menos desde 2022, as entidades com maior adesão, atingindo os 44% em setembro de 2025. Seguem-se, com valores bastante próximos entre si, à data de setembro de 2025, os domínios associados às empresas cotadas no PSI 20 e os 250 domínios mais visitados com nome de domínio de topo ".PT". Estes três grupos apresentam taxas de adesão acima das observadas nos 1000 domínios mais visitados a nível mundial (cerca de 11,8%), valor quase idêntico ao dos domínios associados a câmaras municipais (11,7%). Em último lugar, com valores abaixo dos 5%, encontramos os órgãos de comunicação social nacionais.

Figura 42

PERCENTAGEM DE ADOÇÃO DE DNSSEC



Fonte: ISOC-PT

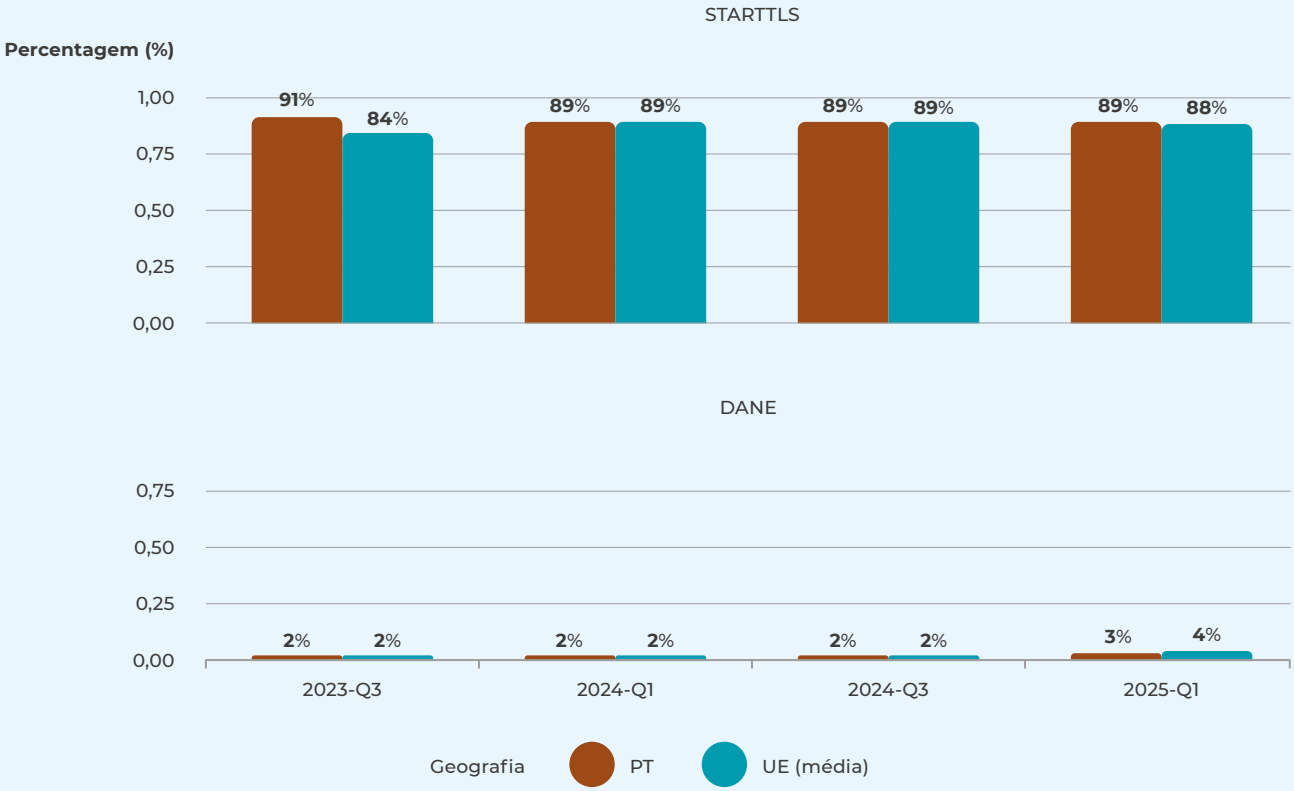
Para analisar a segurança ao nível das comunicações por *email*, foi tido em conta a implementação do comando StartTLS, que ativa, e o protocolo *DNS-based authentication of named entities* (DANE) que garante a autenticidade dos certificados TLS. Enquanto o primeiro ativa o protocolo de encriptação TLS para a transmissão de *emails*, o segundo verifica se os certificados TLS utilizados são autênticos[19]. Recorrendo aos dados do projeto KISDM é possível verificar que as taxas de adoção destas tecnologias são bastantes estáveis ao longo do tempo, tanto a nível nacional como europeu. Existem diferenças substanciais, no entanto, na magnitude da taxa de adoção. Enquanto o StartTLS apresenta taxas de adoção perto dos 89% em Portugal e na UE, o protocolo DANE ronda apenas os 3%. É importante sublinhar que a baixa taxa de adoção deste protocolo de segurança não se limita ao espaço da UE, sendo também observada noutras geografias[20]. Estes resultados estão relacionados com a baixa adoção do DNSSEC, sendo este último uma condição necessária para a implementação do DANE.

19 Ver recomendação técnica do CNCS, disponível em: https://www.cncs.gov.pt/docs/cncs-rt-0121-starttls-dane.pdf

20 Ver relatório de Kouliaridis & Kounelis (2025b).

Figura 43

PERCENTAGEM DE ADOÇÃO DE STARTTLS E DANE



Fonte: DG Connect/JRC

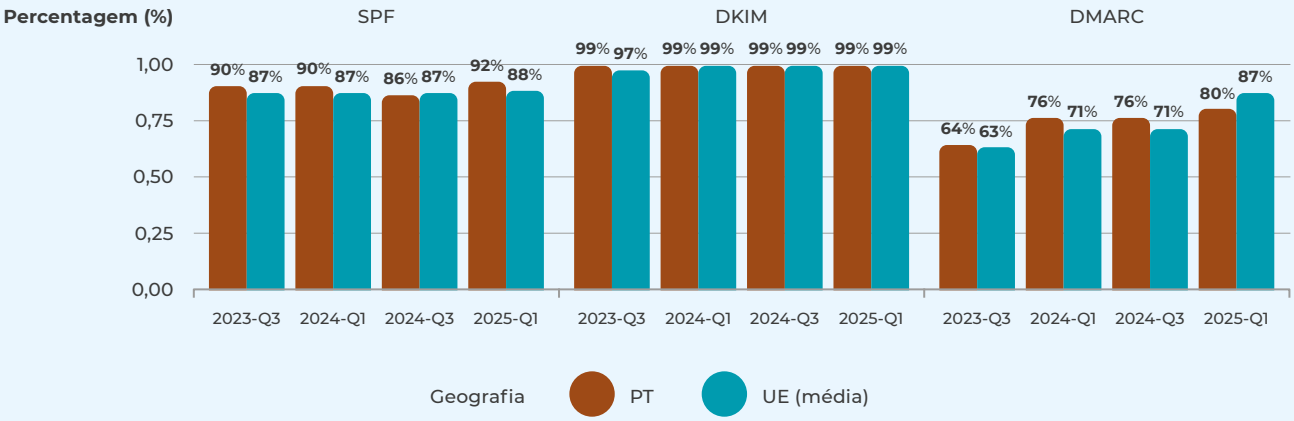
É normalmente através de mensagens eletrónicas de *email* que algumas das ciberameaças mais relevantes em Portugal se materializam, como é o caso da engenharia social e o *phishing*. Existem vários métodos e protocolos técnicos que procuram dar resposta a estas e outras ações maliciosas, nomeadamente o registo *Sender Policy Framework* (SPF) e os métodos de autenticação *DomainKeys Identified Mail* (DKIM) e *Domain-Based Message Authentication, Reporting and Conformance* (DMARC)[21]. Em conjunto, estes elementos constituem um obstáculo importante para os atacantes que procuram imitar domínios legítimos e de confiança para realizar esses ciberataques. Isto é, sem a implementação as tecnologias DNMARC, SPF e DKIM o servidor de destino da mensagem eletrónica não consegue proceder à verificação da autenticidade do nome de domínio utilizado pelo remetente.

Com base nos dados do projeto KISDM é possível constatar a existência de elevadas taxas de adoção destas tecnologias em Portugal e na UE. A implementação do DKIM é quase total em Portugal, tendo-se mantido relativamente estável ao longo do período observado. Igualmente, a adoção de SPF no primeiro trimestre de 2025 foi muito elevada, a rondar os 92%, estando 4 pp acima da média da UE, padrão que se observa desde o terceiro trimestre de 2023. Observam-se, contudo, taxas de adoção bastante mais moderadas no caso da implementação do DMARC. No terceiro trimestre de 2023, a adoção em Portugal e na UE (média) rondava os 64%. Ainda assim, desde 2023 que se tem observado um crescimento significativo na implementação do DMARC. No primeiro trimestre de 2025, a adesão era de 80% em Portugal, o que representa uma subida de 16 pp desde 2023, e 87% na média da UE, um aumento de 24 pp.

21 Ver recomendação técnica do CNCS, disponível em: https://www.cncs.gov.pt/docs/cncs-rt0119-spf-dkim-dmarc-v2.pdf

Figura 44

TAXA DE ADOÇÃO (%) DE SPF, DKIM E DMARC

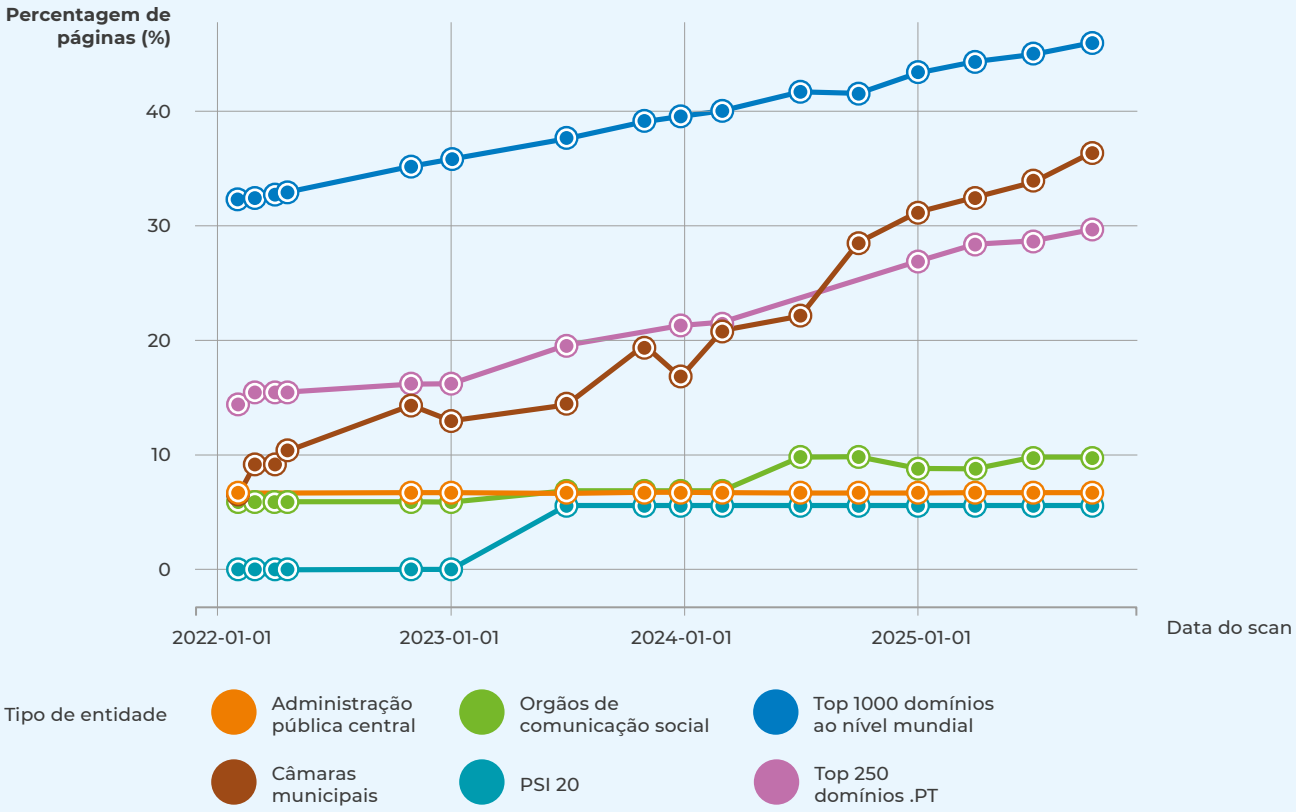


Fonte: DG Connect/JRC

É possível analisar a adoção destas tecnologias tendo em conta o tipo de nome de domínio de *email* com recurso a dados do ISOC-PT, que considera estas métricas de forma conjunta sob a classificação de "medidas de proteção *antiphishing*". Os nomes de domínios mais visitados a nível mundial, utilizados aqui como grupo de controlo, parecem recorrer com bastante mais frequência, em relação aos outros grupos analisados, a medidas de proteção contra o *phishing*, com 46% em setembro de 2025, uma tendência que é observada desde 2022. Os nomes de domínio associados a câmaras municipais parecem ser aqueles que apresentam a maior adesão dentro dos grupos analisados nacionais desde, pelo menos, o segundo trimestre de 2024, com 36%, em setembro de 2025. Em segundo lugar, encontra-se os 250 nomes de domínios mais populares ".PT" com uma adesão a medidas de proteção *antiphishing* na ordem dos 30%. Estes dois grupos registaram melhorias notáveis na adoção destas medidas, aumentando, respetivamente, 30 pp e 15 pp. Contudo, as taxas de adesão mais baixas, de respetivamente 7% e 6%, e sem grande evolução ao longo do período observado, surgem em relação às entidades da administração pública central e nos nomes de domínio associados às empresas do PSI 20. Isto é particularmente notório já que, como demonstra o Relatório ReC de 2025, a marca destas entidades é frequentemente utilizada em ataques de *phishing* (CNCS, 2025, p. 34-35).

Figura 45

PERCENTAGEM DE DOMÍNIOS A ADOTAR MEDIDAS ANTIPHISHING



Fonte: ISOC-PT

EM PORTUGAL, 68% DAS EMPRESAS CONSIDERARAM QUE DIFICULDADES DE RECRUTAMENTO AUMENTARAM A SUA EXPOSIÇÃO A INCIDENTES

E. CIBER-RESILIÊNCIA

À medida que os riscos e ameaças no ciberespaço se tornam, cada vez mais, parte da realidade quotidiana da nossa sociedade, a cibersegurança deixou de se focar apenas na prevenção dos ciberataques – diminuindo a superfície de ataque – para incluir a capacidade de limitar as suas consequências, assim como garantir uma rápida recuperação e integração de lições aprendidas. Este conjunto de capacidades define aquilo que normalmente se entende por "ciber-resiliência" (Sepúlveda et al., 2020). Utilizado essencialmente em contexto técnico-organizacional, mais recentemente este conceito tem vindo a ser também utilizado para analisar o nível e capacidades em cibersegurança de países[22] e indivíduos (Joinson et al., 2023).

Neste capítulo, analisam-se alguns dos fatores que contribuem para a ciber-resiliência da sociedade portuguesa. Desde logo, procurou-se analisar o interesse dos portugueses em relação a termos relacionados com a cibersegurança como forma de aferir o seu interesse pelas ciberameaças e conhecer as suas perceções de risco na utilização e tecnologias digitais. De seguida, foi analisado o nível de investimento das organizações em capacitação humana e tecnológica em cibersegurança, uma condição indispensável para garantir um bom nível de ciber-resiliência. Finalmente, olhamos para as ações de sensibilização e educação. Tornou-se recorrente afirmar que não existem profissionais suficientes na área para suprir as necessidades do mercado. Nesse sentido, e apesar da obtenção de diplomas universitários não ser a única via para a desenvolver conhecimentos especializados em cibersegurança, é muito importante não perder de vista a evolução positiva da oferta de formações nas universidades e politécnicos em Portugal.

22 Ver, por exemplo, o *National Cyber Security Index* da e-Governance Academy, disponível em: https://ncsi.ega.ee/

CONHECIMENTO DA AMEAÇA

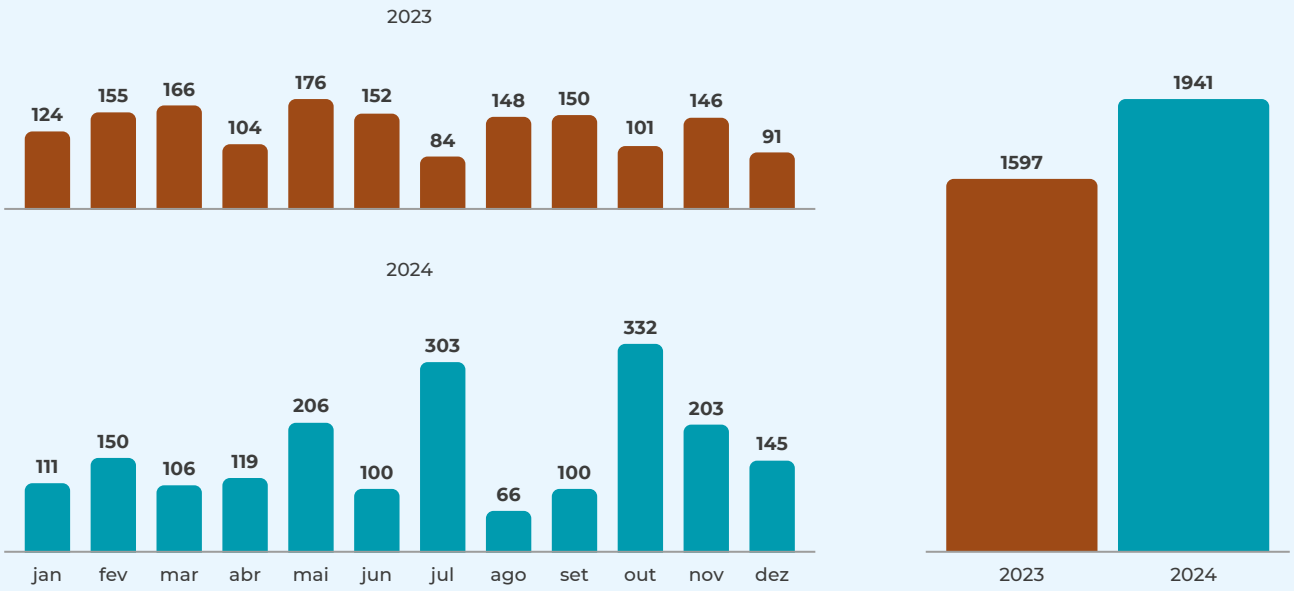
Para garantir a resiliência face às ciberameaças é essencial primeiro conhecê-las. Para analisar a saliência da cibersegurança e das principais ciberameaças na sociedade portuguesa, recorremos nesta subsecção a dados relativos à cobertura mediática e volume de pesquisas *online* realizadas sobre estas matérias.

Através da plataforma *Media Cloud* é possível analisar o número de artigos *online* que foram publicados por órgãos de comunicação social em Portugal que mencionaram o termo "cibersegurança" (Roberts et al., 2021). Contrariamente ao observado em 2023, onde o número de artigos a mencionar este termo era inferior ao do ano anterior, o número de artigos a mencionar a cibersegurança aumentou significativamente em 2024, passando de 1597 para 1941, resultando num aumento de aproximadamente 22%.

Analisando a série temporal, parece existir, à semelhança de outros anos, uma cobertura mediática reativa, caracterizada por uma correlação temporal entre a cobertura mediática da cibersegurança e os incidentes com maior impacto nacional ou internacional. Verifica-se que outubro – definido como mês europeu da cibersegurança desde 2012 – foi o mês com mais artigos a mencionar o termo, coincidindo com um incidente de *ransomware* contra uma entidade da administração pública central que, por fornecer um serviço de autenticação essencial tanto para organismos públicos e privados como para os cidadãos, teve repercussões em todo o país. Seguindo-se o mês de julho, marcado por um erro na atualização de um *software Endpoint Detection and Reaction* de uma empresa de cibersegurança sediada nos Estados-Unidos da América que causou indisponibilidades massivas de serviços à escala global.

Figura 46

DISTRIBUIÇÃO DO NÚMERO DE ARTIGOS DE MEIOS DE COMUNICAÇÃO SOCIAL COM O TERMO "CIBERSEGURANÇA"



Fonte: Mediacloud

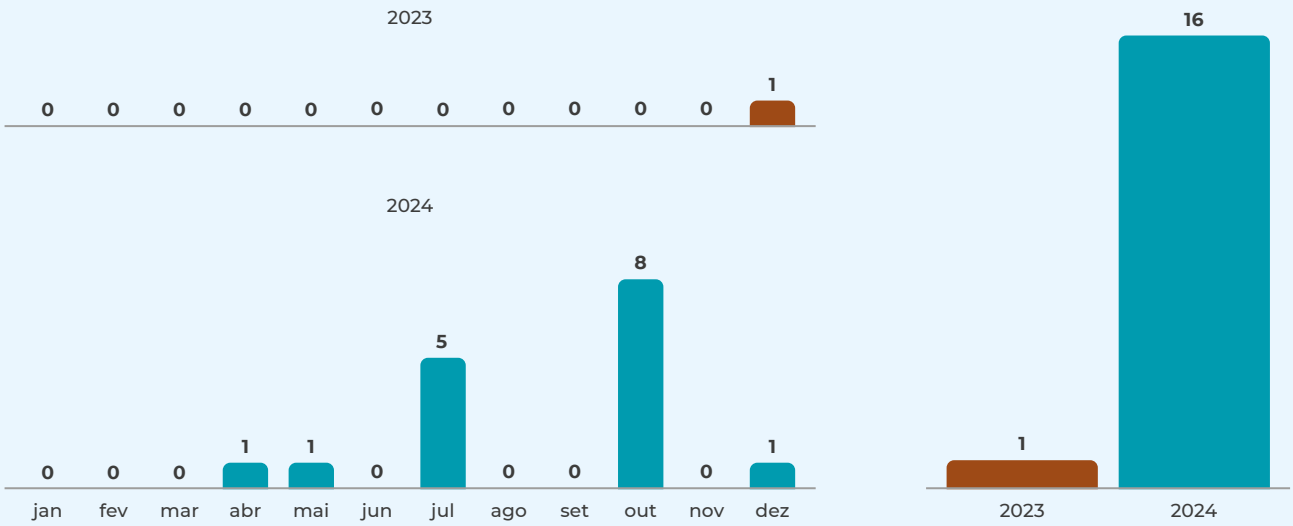
O PAPEL DA COMUNICAÇÃO SOCIAL PARA CIBERSEGURANÇA NA SOCIEDADE

Estudos académicos recentes demonstram que a comunicação social, a par das redes sociais, família e amigos próximos, continua a ser das principais fontes de informação sobre cibersegurança para os indivíduos (Herbert et al., 2024). Nesse sentido, é possível afirmar que uma maior cobertura mediática da cibersegurança e ciberameaças contribui para uma maior consciência do público para estes temas sem que, no entanto, se possa concluir que esta se traduz na adoção de medidas de segurança por parte dos indivíduos. Estudos recentes colocam ainda em evidência, de forma consistente, que a discussão pública e cobertura mediática destes temas tendem a focar-se mais nos eventos e ciberameaças do que na discussão das medidas de proteção a adotar (Meissner et al., 2025; Quinlan et al., 2024; Alagheband et al., 2020).

É importante referir que a forma como os órgãos de comunicação tratam os incidentes de *ransomware* tem impacto no sucesso dos grupos de cibercriminosos por detrás deste tipo de ciberataques. Contrariamente a outras ciberameaças, como os atores estatais (*Advanced Persistente Threats* ou APT), os grupos de *ransomware* beneficiam, em grande medida, da publicidade gerada pela cobertura mediática. Esta permite-lhes reforçar a sua reputação em relação a outros grupos rivais e junto do público em geral, potenciando, assim, o pagamento de resgates. Isto significa que para lutar de forma eficaz contra o *ransomware* não é suficiente provocar a disrupção das operações dos grupos, reforçar a partilha de informações ou reforçar a resiliência das redes e sistemas de informação. São também necessárias ações focadas na promoção de uma cobertura mediática particularmente responsável, por exemplo, através do desenvolvimento de códigos de ética e formação especifica para jornalistas (Smeets, 2025).

Figura 47

DISTRIBUIÇÃO DO NÚMERO DE ARTIGOS DE MEIOS DE COMUNICAÇÃO SOCIAL COM O TERMO "INFOSTEALER"



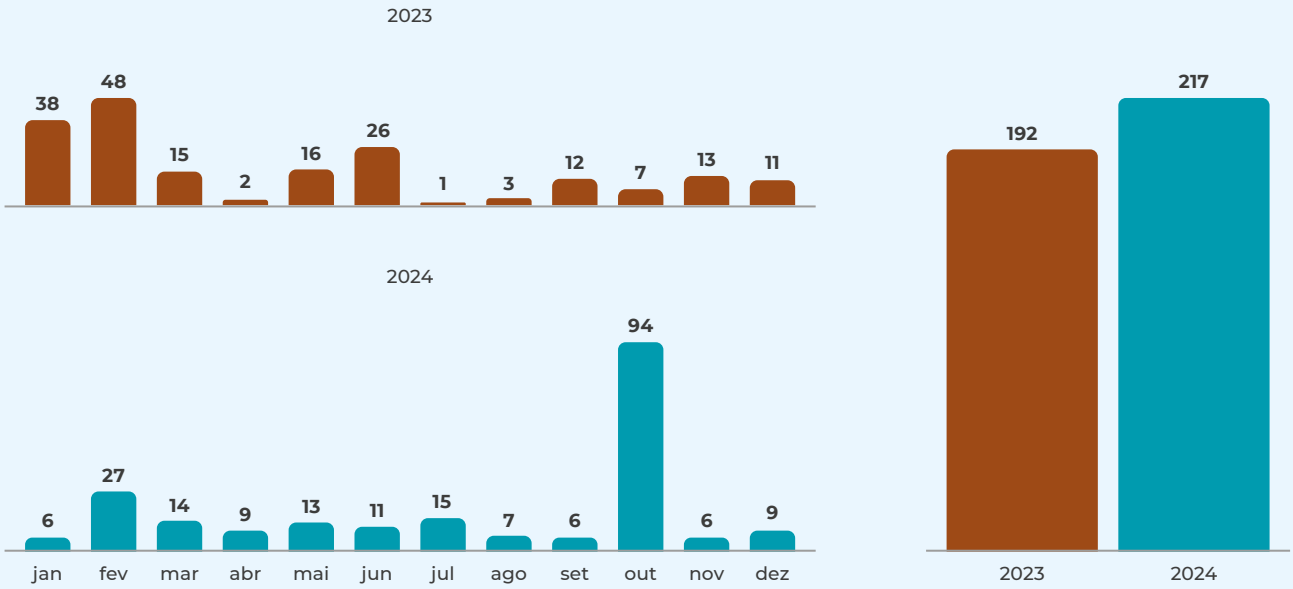
Fonte: Mediacloud

Analisando agora uma outra tendência central em 2024, a ameaça dos *infostealers*, verifica-se que, embora este termo (e variantes) apenas tenha sido identificado num artigo na nossa amostra relativa a 2023, em 2024 verifica-se um aumento significativo do número de artigos publicados em órgãos de comunicação social que mencionam "*infostealers*". Esse aumento é particularmente notório em outubro, coincidindo com um debate público sobre a possível relação entre a divulgação de dados pessoais de utilizadores da plataforma de uma entidade da administração pública central e a indisponibilidade de serviços provocada por um ciberataque de *ransomware* noutra entidade do mesmo setor nesse mesmo mês.

O número de artigos a mencionar "*ransomware*" aumentou 13% em 2024, relativamente a 2023, atingindo os 217 artigos. Este aumento parece dever-se, sobretudo, ao mês de outubro, no qual foram publicados aproximadamente 47% de todos os artigos publicados nesse ano a mencionar o termo. Facto coincidente com o incidente de *ransomware* de grande impacto mencionado acima.

Figura 48

DISTRIBUIÇÃO DO NÚMERO DE ARTIGOS DE MEIOS DE COMUNICAÇÃO SOCIAL COM O TERMO "RANSOMWARE"



Fonte: Mediacloud

Embora não seja trivial medir o interesse da sociedade portuguesa em matérias relacionadas com a cibersegurança, uma análise dos hábitos de pesquisa *online* pode-nos ajudar a aproximar essa realidade. Para analisar estes dados recorremos à plataforma *Google Trends* que fornece dados que medem o volume relativo das pesquisas no motor de busca Google associado a um termo, normalizado pelo valor total das pesquisas numa certa geografia e num determinado intervalo de tempo. O resultado é um índice de 0 a 100 que aproxima a popularidade relativa de um certo termo de pesquisa relativamente a outros pesquisados em contexto semelhante.

À semelhança do que foi observado na análise da cobertura mediática, nota-se um maior interesse relativo pelo termo "cibersegurança" nas pesquisas em 2024 relativamente a 2023. Verificou-se uma maior popularidade em 2024 (média de 39,8) do que em 2023 (média de 32). Tal como se observou acima, o volume relativo de pesquisas revela um maior interesse na cibersegurança no mês de outubro (média de 60), quase 16 pontos acima do segundo mês com maior volume em 2024.

Figura 49

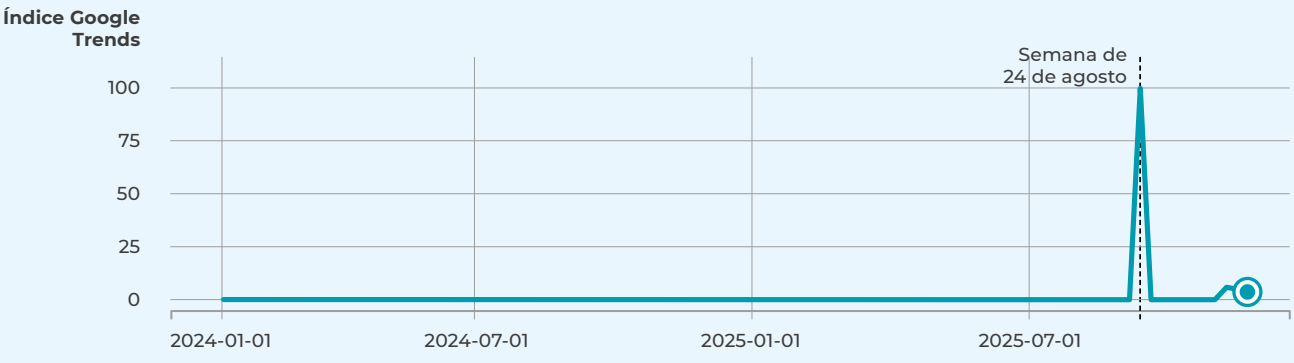
DISTRIBUIÇÃO DE VOLUME RELATIVO DE PESQUISAS PARA O TERMO "CIBERSEGURANÇA"

Fonte: Google Trends

Particularmente interessante parece ser o resultado da análise do volume de pesquisas para o termo *smishing*, uma ameaça central em 2024 e 2025. Embora o volume relativo de pesquisas para este termo seja 0 desde 2023, na semana de 24 de agosto de 2025, o índice de pesquisas para este termo atinge subitamente o valor máximo do indicador, 100, para a semana em questão. Isto é significativo, já que o segundo e terceiro maior valor atingido nas pesquisas deste termo são respetivamente 6 e 5. Cumpre destacar que este período, assim como as semanas que o antecederam e precederam, coincidiu com volumosas campanhas de *smishing* em vários setores, tais como a banca e retalho, tendo recebido uma cobertura mediática relevante.

Figura 50

DISTRIBUIÇÃO DE VOLUME RELATIVO DE PESQUISAS PARA O TERMO "SMISHING"



Fonte: Google Trends

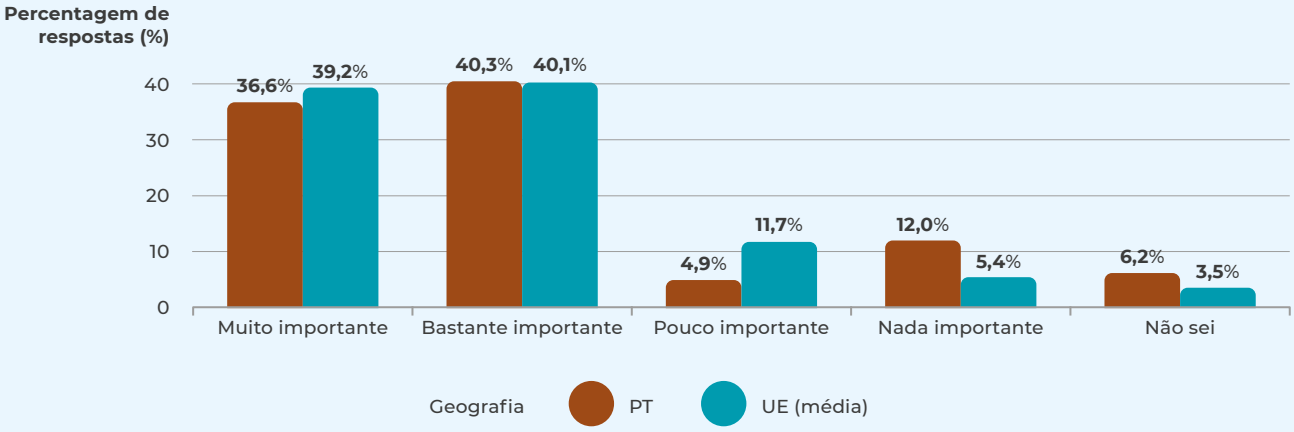
Analisado o termo "DDoS", parece ter havido um ligeiro aumento na ordem dos 2 pontos na média deste índice entre 2023 e 2024. Outubro é, mais uma vez, o mês com mais pesquisas em 2024, distanciando-se a 10 pontos do segundo mês com maior valor no índice (julho), pico potencialmente associado a um ataque de DDoS contra uma famosa plataforma de arquivo de páginas da internet a nível global.

Até agora analisámos o conhecimento da ameaça de um ponto de vista estritamente focado na saliência do tema. A perceção do nível de ameaça de certos comportamentos ou serviços críticos para a cibersegurança oferece-nos também uma outra forma de medir o conhecimento da ameaça na sociedade portuguesa. Cumpre relembrar que esta perceção pode não estar necessariamente alinhada com o nível de ameaça real e que, por isso, estes resultados não devem ser interpretados de forma normativa.

Com base em dados do inquérito da década digital do Eurobarómetro (Eurobarometer, 2025b), analisamos primeiro a perceção do impacto de melhorias na cibersegurança na utilização diária de tecnologias digitais. Cerca de 37% dos inquiridos portugueses consideraram que as melhorias na cibersegurança foram muito importantes para a utilização diária de tecnologias digitais, face a 39% da média da UE; cerca de 40%, tanto em Portugal como na média da UE, consideraram que estas foram importantes. Estes dados sugerem um reconhecimento, ainda que implícito, das ciberameaças e do papel da cibersegurança no seu combate.

Figura 51

PERCEÇÃO DO IMPACTO DE MELHORIAS NA CIBERSEGURANÇA NA UTILIZAÇÃO DIÁRIA DE TECNOLOGIAS DIGITAIS

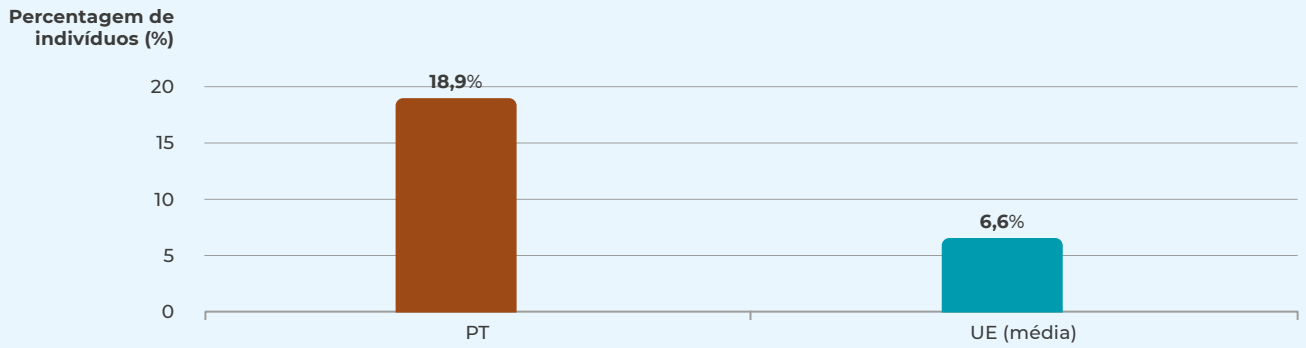


Fonte: Eurobarómetro

Os portugueses também parecem demonstrar uma maior reticência na utilização de certas tecnologias por motivos de cibersegurança, o que, embora não seja algo em si positivo do ponto de vista da digitalização, sugere a consciência da existência de riscos e ameaças associados à sua utilização. Em 2024, 19% dos indivíduos em Portugal consideravam não utilizar sistemas IoT por preocupações relacionadas com cibersegurança, nomeadamente por temerem o comprometimento do dispositivo (Eurostat, 2024h). Este valor é significativamente superior à média europeia que se situa em 7% e sendo Portugal apenas superado pela Finlândia (26%), Espanha (21%) e Áustria (20%).

Figura 52

PERCENTAGEM DE INDIVÍDUOS QUE NÃO UTILIZA DISPOSITIVOS/SISTEMAS IOT DEVIDO A PREOCUPAÇÕES COM A CIBERSEGURANÇA

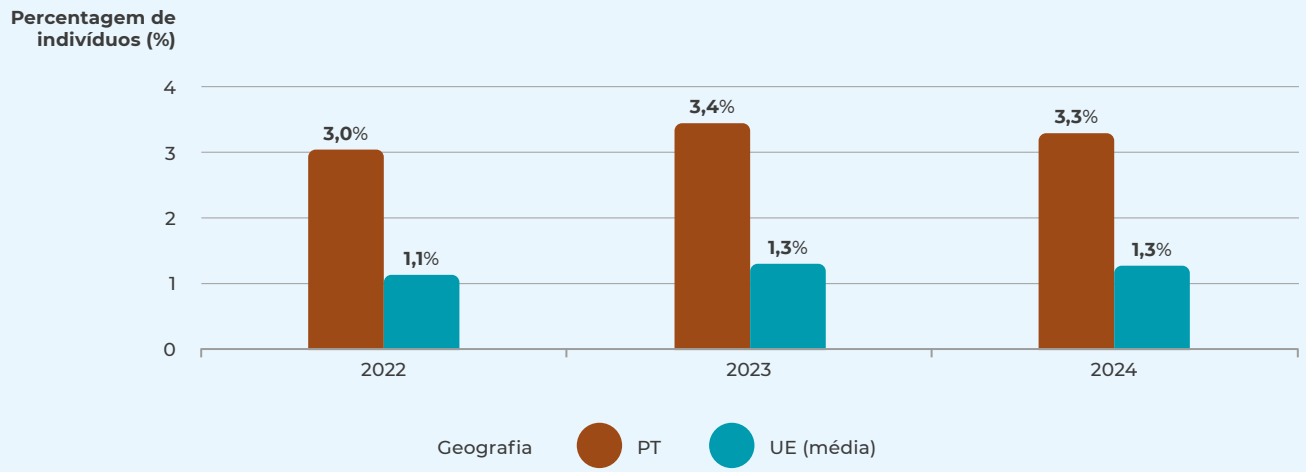


Fonte: Eurostat

A perceção da existência de ameaças associadas à utilização da tecnologia pode estar a ter algum impacto na utilização de serviços digitais da administração pública. Segundo dados do Eurostat, o número de indivíduos que não requisitaram documentos ou submeteram pedidos a entidades da administração pública, através da internet, tem estado acima da UE desde, pelo menos, 2022. Em 2024, aproximadamente 3% dos indivíduos, em Portugal, afirmam não recorrer a serviços digitais da administração pública por motivos de segurança (Eurostat, 2024i). Apesar destes valores poderem parecer baixos, é importante salientar que esta resistência parece ser significativa: Portugal é o segundo país da UE com a maior percentagem de indivíduos a não recorrer a estes serviços por motivos de segurança, sendo ultrapassado apenas por França.

Figura 53

PERCENTAGEM DE INDIVÍDUOS QUE NÃO UTILIZOU SERVIÇOS DIGITAIS DA ADMINISTRAÇÃO PÚBLICA/ GOVERNAMENTAIS POR PREOCUPAÇÕES COM A CIBERSEGURANÇA

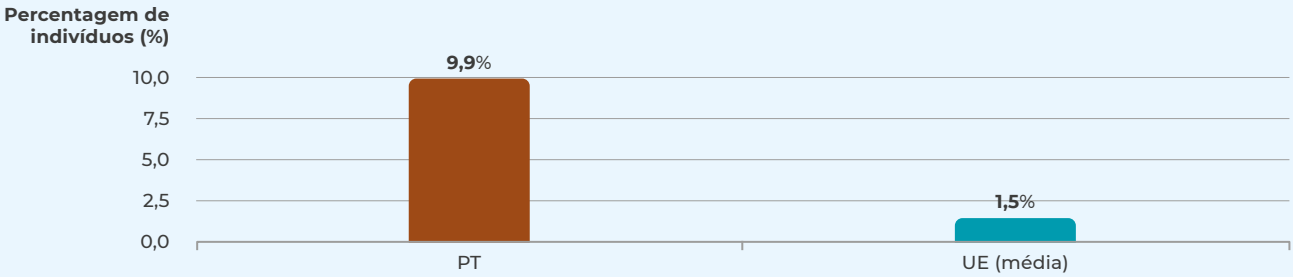


Fonte: Eurostat

Observamos o mesmo padrão quando analisamos o número de indivíduos a não utilizar, nos últimos 12 meses, tecnologias de identidade digital (eID) por motivos de segurança (Eurostat, 2023e). Em 2023, aproximadamente 10% dos inquiridos portugueses não tinha utilizado estas tecnologias recentemente "porque não se sentiam seguros ao fazê-lo", um valor 8,4 pp acima da média europeia, sendo Portugal o país com a percentagem mais elevada dos 27.

Figura 54

PERCENTAGEM DE INDIVÍDUOS QUE NÃO UTILIZOU EID POR PREOCUPAÇÕES COM A CIBERSEGURANÇA

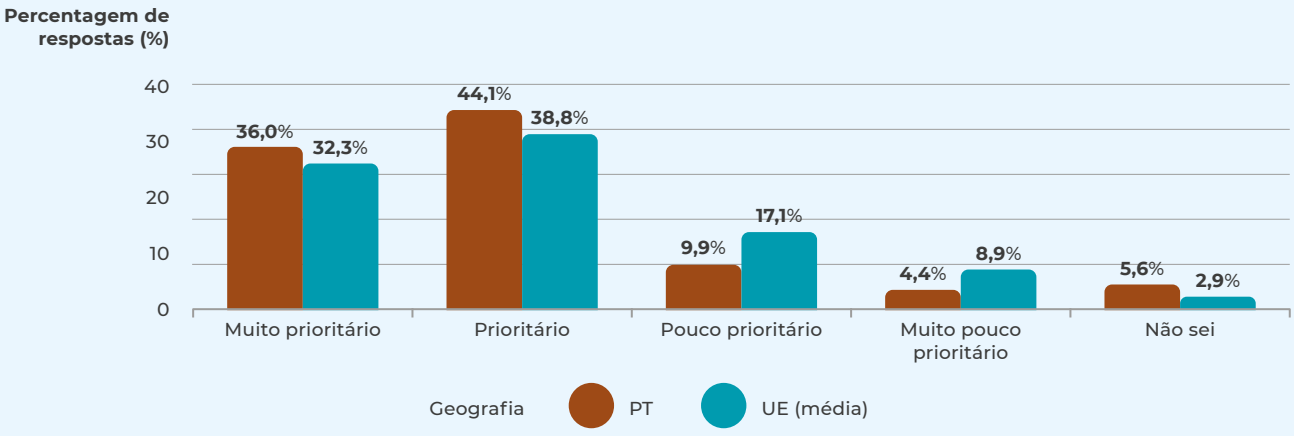


Fonte: Eurostat

Analisado agora a perceção da ameaça no contexto empresarial, recorremos aos dados do inquérito do Eurobarómetro *Cyberskills*, de maio de 2024, onde se perguntou às empresas qual o grau de prioridade atribuído à cibersegurança nas suas atividades (Eurobarometer, 2024). No segundo trimestre de 2024, as empresas portuguesas pareciam dar uma maior importância à cibersegurança em comparação com as suas congéneres europeias. Cerca de 36% das empresas inquiridas classificaram a cibersegurança com uma prioridade muito elevada e 44% como sendo uma área prioritária, valores que superam a média da UE, onde se registam 32% e 39%, respetivamente.

Figura 55

AVALIAÇÃO DA CIBERSEGURANÇA ENQUANTO PRIORIDADE PARA AS EMPRESAS



Fonte: Eurobarómetro

CAPACITAÇÃO

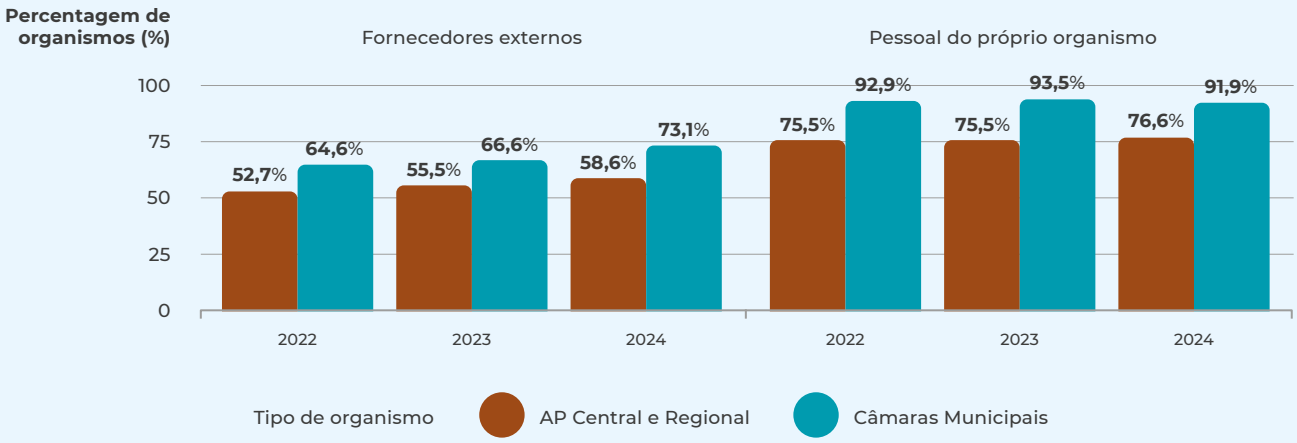
Apesar das medidas organizativas implementadas pelas organizações, os incidentes de cibersegurança têm aumentado tanto na sua frequência como complexidade. Perante este quadro de ameaça, a capacitação das organizações, seja de uma perspetiva técnica, humana ou processual, torna-se crucial. Com base em dados de várias fontes, vamos analisar, abaixo, o investimento, tanto financeiro como na capacitação humana, feito pelas organizações no âmbito da gestão da sua cibersegurança.

Com base em dados de um inquérito do Eurobarómetro, de maio de 2024, *Cyberskills*, analisamos o estado da capacitação das organizações na vertente humana (Eurobarometer, 2024). As empresas em Portugal recorrem mais a indivíduos ou empresas externas à organização para tratarem de aspetos ligados à cibersegurança, atingindo os 60% das empresas, face aos 51% da média da UE.

Já na administração pública, os dados da DGEEC revelam que as tarefas de cibersegurança continuam sobretudo a ser prestadas por funcionários do próprio organismo, por oposição à contratação de serviços externos. Isto é particularmente notório no caso dos organismos municipais, onde o aproximadamente 92%, em 2024, dos inquiridos respondeu neste sentido. Na administração pública central/regional aproximadamente 77% dos organismos inquiridos, à data de 2024, considerou que estas tarefas eram prestadas por trabalhadores internos. Embora os valores se tenham mantido relativamente estáveis desde 2023, parece existir uma ligeira tendência de aumento no número de prestadores externos a prestarem serviços de cibersegurança, tendo-se observado um moderado, mas constante, aumento na percentagem de organismos, tanto da administração pública central/regional (59% em 2024) como nas câmaras municipais (73% em 2024) que procuram este tipo de serviços junto de prestadores externos.

Figura 56

PRESTAÇÃO DE SERVIÇOS DE CIBERSEGURANÇA NA AP



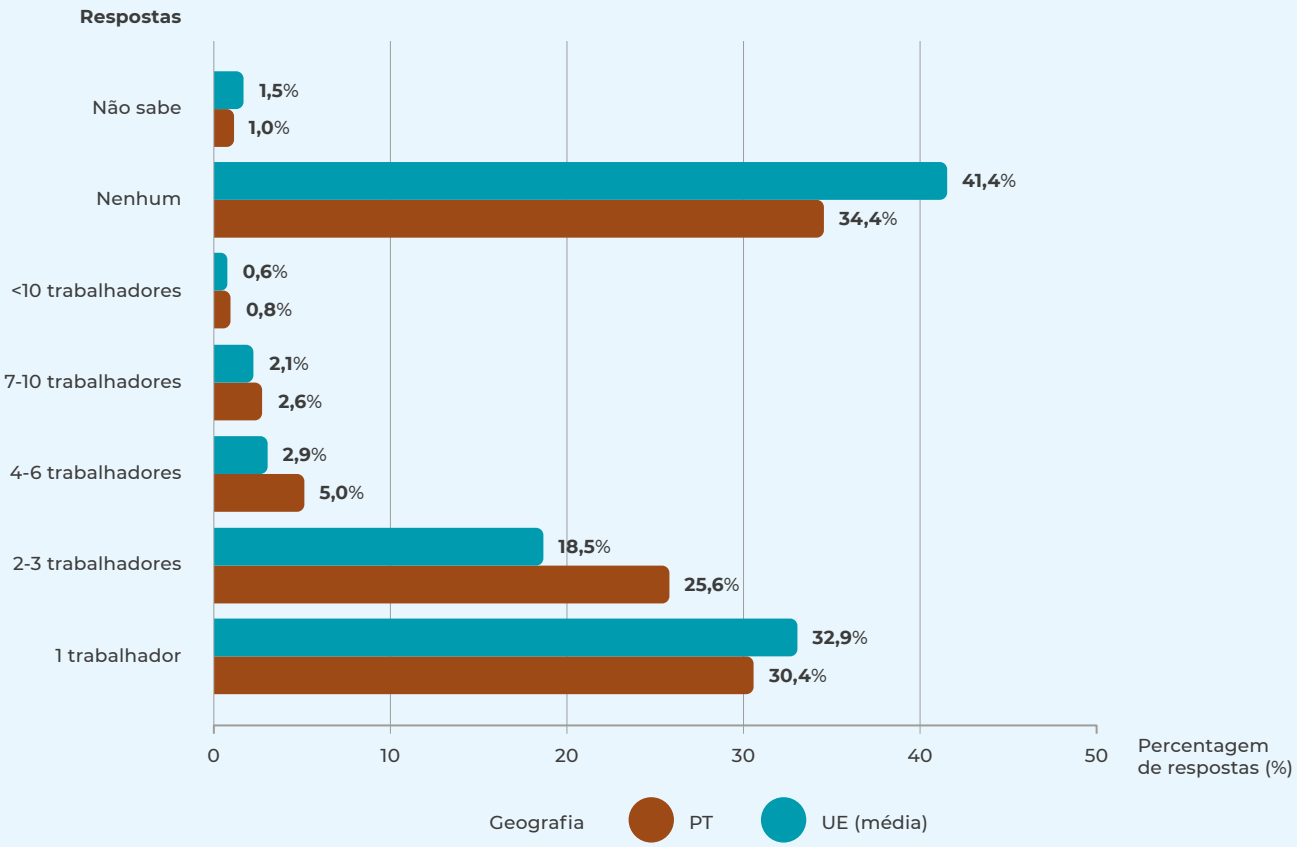
Fonte: DGEEC

Nas empresas que têm trabalhadores com funções relacionadas com a cibersegurança, cerca de 64% das empresas em Portugal têm pelo menos 1 funcionário a executar tarefas de cibersegurança, enquanto a média da UE ronda os 57%. Cerca de 26% das empresas em Portugal têm 2-3 colaboradores, valor 7 pp acima da média da UE.

Cerca de 59% destes trabalhadores absorveram estas tarefas no seu cargo não diretamente relacionado com cibersegurança (e.g. com suporte de TIC), tendência alinhada com a média da UE (57%). Ao nível da contratação, 40% dos trabalhadores com tarefas em cibersegurança foram contratados sem que a sua função anteriormente exercida estivesse relacionada com cibersegurança (média da UE é de 34%), enquanto apenas 19% foram recrutados nessa área. Verifica-se também que 19% das empresas portuguesas, e 17% das europeias, contrataram trabalhadores para posições relacionadas com cibersegurança como primeiro emprego.

Figura 57

NÚMERO DE TRABALHADORES COM FUNÇÕES RELACIONADAS COM A CIBERSEGURANÇA

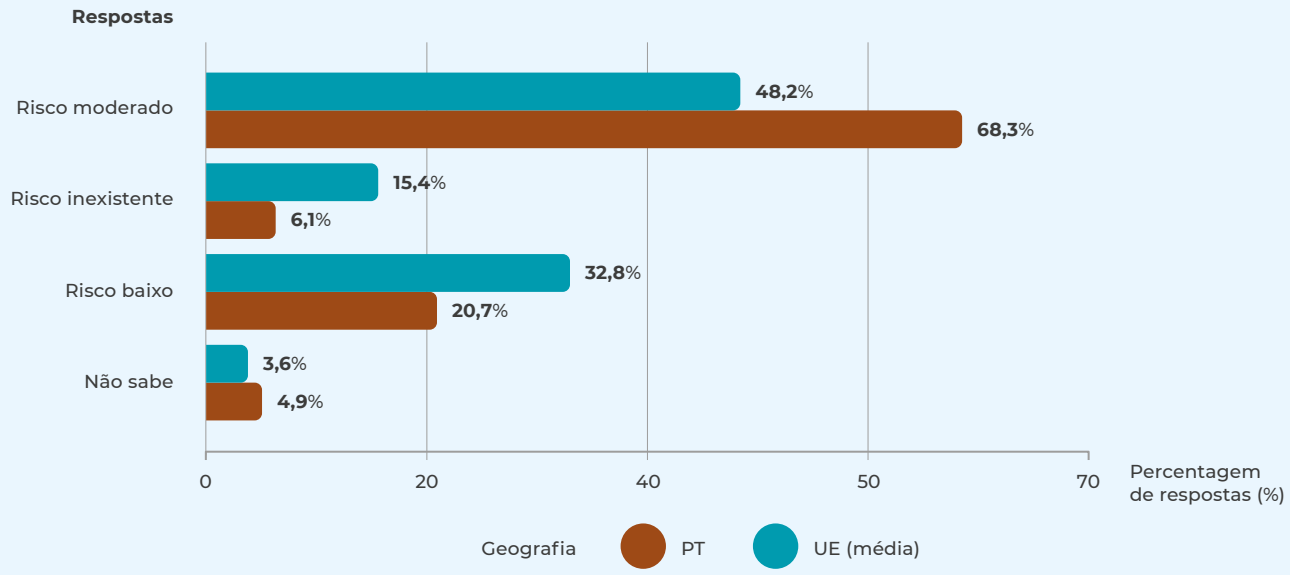


Fonte: Eurobarómetro

Em Portugal, 16% das empresas consideraram, nos últimos 12 meses, difícil contratar profissionais com as competências adequadas para executar tarefas relevantes na área da cibersegurança. Alguns obstáculos são comuns ao resto da Europa, como a falta de candidatos, identificado por 51% das empresas que não conseguiram contratar em Portugal e 44% na média da UE; assim como a dificuldade em encontrar candidatos qualificados (40% em Portugal face a 45% na média da UE). Contudo, alguns entraves parecem ser mais desafiantes para as empresas portuguesas. Cerca de 37% das empresas inquiridas em Portugal consideraram que a falta de conhecimento sobre as competências necessárias e funções relevantes na área da cibersegurança foi um obstáculo importante no momento de recrutar, valor aproximadamente 15 pp acima da média da UE. Além disso, 29% das empresas inquiridas portuguesas consideraram que os requisitos de credenciação de segurança dificultaram o recrutamento, contra 16% na média da UE. Cerca de 68% destas consideraram que dificuldades de recrutamento aumentaram a sua exposição a incidentes de cibersegurança, valor substancialmente acima da média da UE (48%).

Figura 58

PERCEÇÃO DO IMPACTO DAS DIFICULDADES NA CONTRATAÇÃO NA EXPOSIÇÃO DA ORGANIZAÇÃO AO RISCO



Fonte: Eurobarómetro

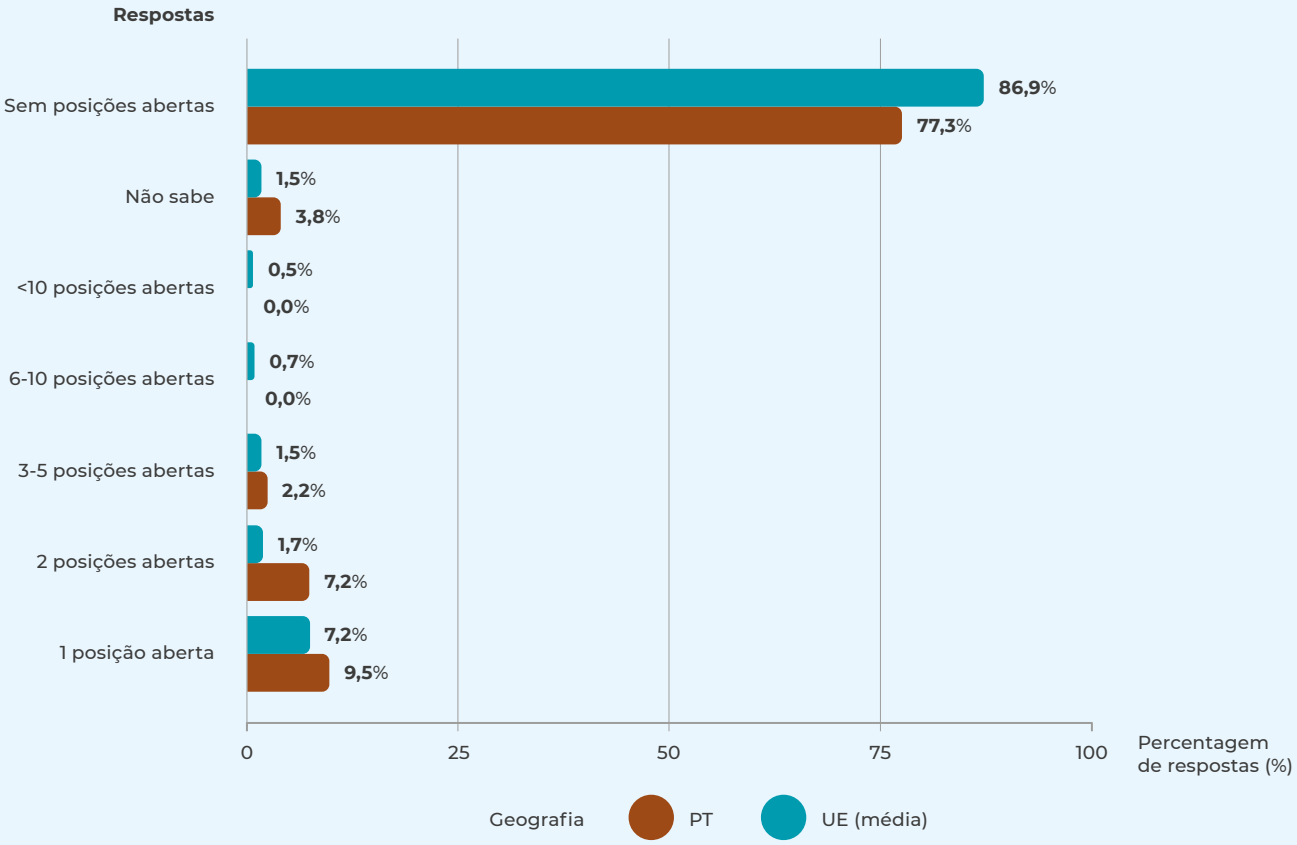
PEDIRAM UM ESPECIALISTA EM CIBERSEGURANÇA?

A cibersegurança abrange uma vasta gama de áreas de especialização, funções e tarefas nas organizações. Para facilitar o desenho de formações e definição e perfis de recrutamento, o CNCS publicou, em 2022, um Referencial de Competências que mapeia as competências e capacidades em cibersegurança (especializadas e transversais), em relação ao Quadro Nacional de Referência para a Cibersegurança, ao Roteiro para as capacidade mínimas de cibersegurança do CNCS e o referencial da *European Cyber Security Organisation*, propondo um método de identificação de necessidades e uma lista de concreta das competências necessárias para executar tarefas nas áreas mais críticas de gestão e operacionalização da cibersegurança numa organização, englobando a gestão de risco, incidentes e desafios organizacionais.

No segundo trimestre de 2024, 77% das empresas portuguesas inquiridas indicaram não ter vagas abertas para o exercício de funções a tempo inteiro especificamente na área de cibersegurança. Este número é inferior à média da UE, que se situa nos 87%. Por outro lado, 10% das empresas portuguesas afirmou ter uma posição aberta na área, superando os 7% registados em média na UE.

Figura 59

PERCENTAGEM DE EMPRESAS COM POSIÇÕES ABERTAS DE CIBERSEGURANÇA



Fonte: Eurobarómetro

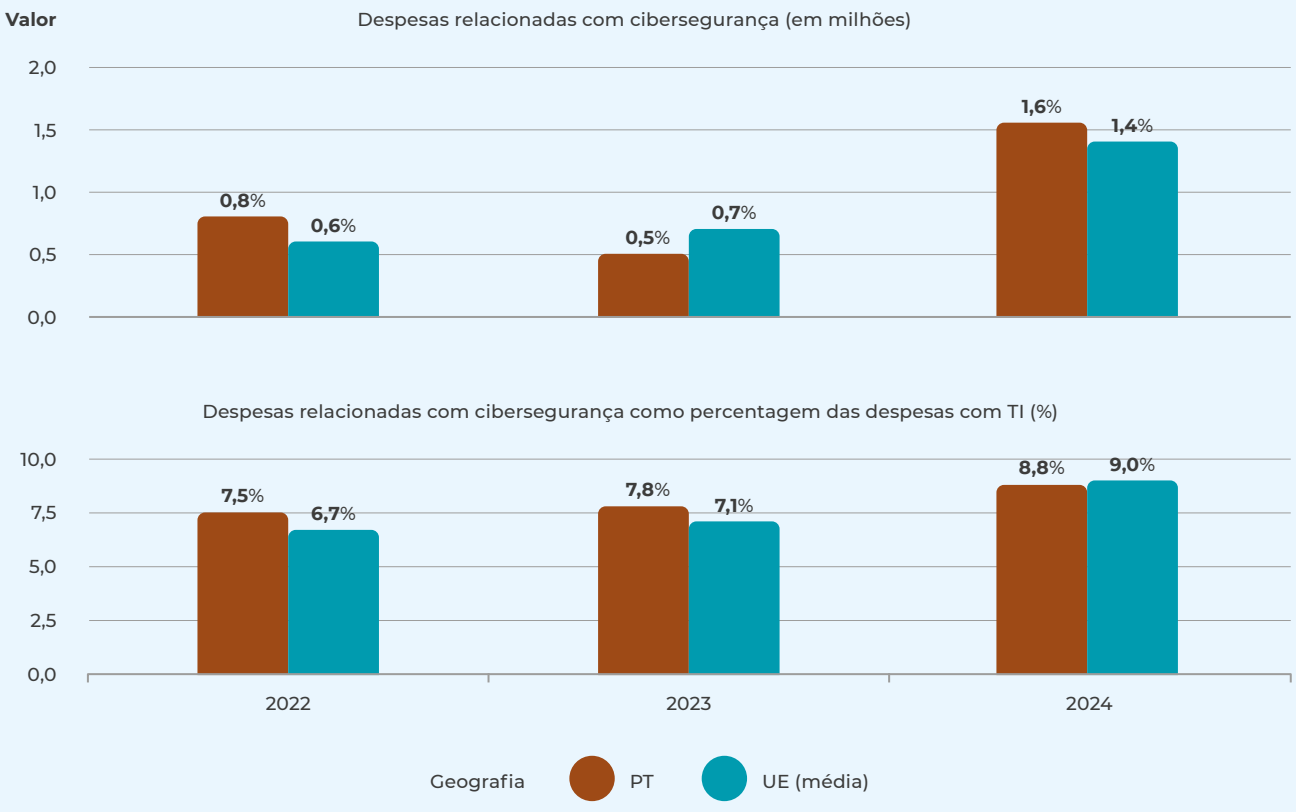
As funções mais valorizadas pelas organizações portuguesas no âmbito da cibersegurança são primariamente as de responsável de cibersegurança/segurança da informação (*Chief Security/Information Officer*), com 47% das empresas portuguesas inquiridas a responderem nesse sentido, face a 17% da média da UE. Do mesmo modo, a função de formador em matérias de segurança parece ser relativamente prioritária para as empresas portuguesas (39%), estando 22 pp acima da média da UE. Seguindo-se as posições de técnico de resposta a incidentes (20% em Portugal e 16% na média da UE), especialista em conformidade legal (18% em Portugal face a 14% na média da UE) e a função de auditor (17% em Portugal e 11% na média da UE).

No que toca às competências consideradas mais importantes por parte das empresas, destacam-se, relativamente à média da UE, a capacidade de identificar e resolver problemas relacionados com a cibersegurança (37% em Portugal face a 20% na UE), a aptidão para analisar, avaliar e rever a segurança de *software* ou *hardware* (33% em Portugal e 21% na média da UE), bem como a capacidade de identificar necessidades de sensibilização, formação e educação nesta área (32% em Portugal face a 15% na média da UE).

Subjacente à capacitação humana, assim como à adoção de medidas organizativas e de tecnologias de cibersegurança, está o investimento económico das organizações na cibersegurança. A ENISA, através de inquéritos desenvolvidos no âmbito da produção do seu relatório anual *NIS Investments*, tem vindo a monitorizar os investimentos feitos por operadores de serviços essenciais e prestadores de serviços digitais, no âmbito da diretiva NIS 1, e, desde 2024, em entidades consideradas essenciais ou importantes, no âmbito da diretiva NIS 2. Em 2022, as despesas medianas relacionadas com cibersegurança por parte de organizações portuguesas rondava os 800 mil euros, valor 200 mil euros acima do valor mediano relativo à UE (ENISA, 2024). Em 2023, observou-se uma queda para um valor mediano de 500 mil euros, não acompanhado pela UE que aumentou 17%. Em 2024, observa-se uma forte recuperação e mesmo aumento no valor mediano investido por parte das organizações portuguesas na ordem dos 220 mil euros, atingindo os 1.7 milhões de euros, valor acima da mediana europeia em 2024 (1.4 milhões de euros). Quando analisamos as despesas relacionadas com cibersegurança enquanto percentagem das despesas com TI, verifica-se um aumento moderado, mas constante, desde 2022, data em que o valor mediano era 7,5% para Portugal e 6,7% na mediana da UE, atingindo, em 2024, os 8,8% em Portugal e 9% na mediana da UE.

Figura 60

DESPESAS COM CIBERSEGURANÇA POR PARTE DE EMPRESAS COBERTAS PELA NIS



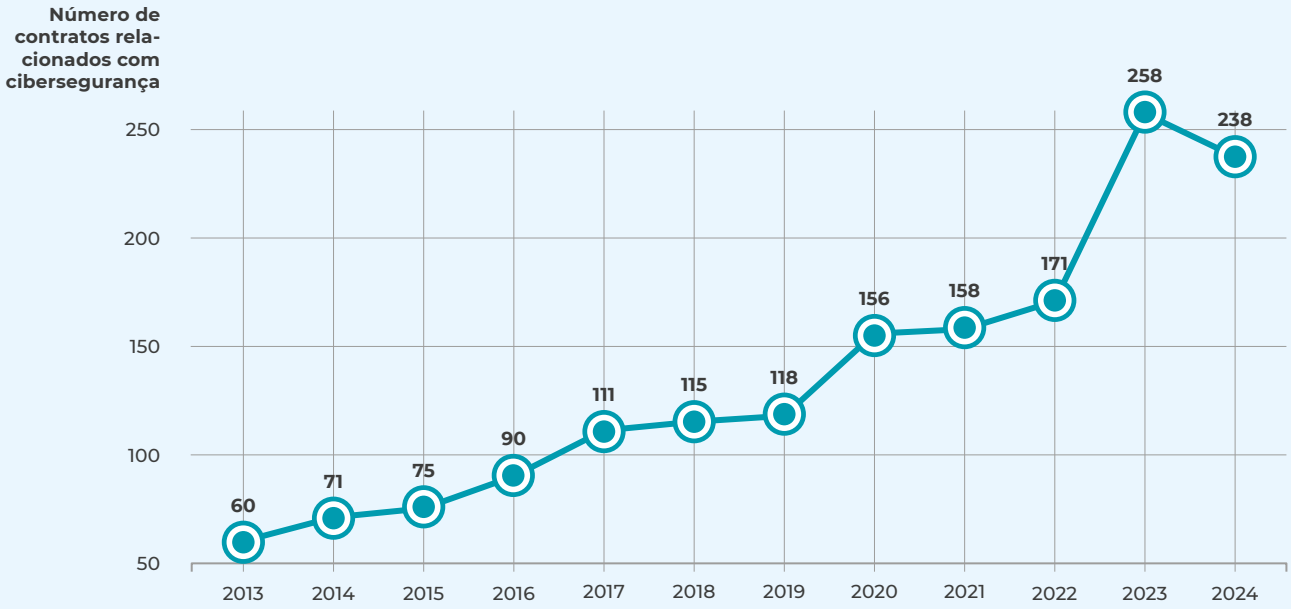
Fonte: ENISA

Para analisar os investimentos em cibersegurança por parte da administração pública, criou-se um conjunto de dados original com informação relativa a contratos públicos, presentes no Portal BASE, relacionados com tecnologias ou serviços tradicionalmente associados à cibersegurança[23]. Mais concretamente, recolhemos informação relativa a contratos públicos entre 2013 e 2024 e depois, recorrendo a 53 expressões regulares relacionadas com 15 tecnologias, serviços ou normas de cibersegurança[24], filtrámos os contratos relevantes com base nas descrições dos objetos contratuais.

O gráfico abaixo revela um crescimento sustentado, quase linear, no investimento em tecnologias e serviços de cibersegurança na administração pública entre os anos de 2013 e 2022. Nota-se, contudo, um salto significativo no número de contratos entre 2022 e 2023, onde se observa um aumento de 51% na contratação de serviços e tecnologias de cibersegurança. Contudo, em 2024, parece ocorrer uma ligeira diminuição na contratação destes serviços e tecnologias, observando-se uma queda de 171 para 258. Entre 2013 e 2024, verificou-se um aumento no número de contratos relacionados com a prestação de serviços ou tecnologias de cibersegurança na ordem dos 296%, facto que sugere uma crescente relevância atribuída à cibersegurança na contratação pública.

Figura 61

NÚMERO DE CONTRATOS PÚBLICOS IDENTIFICADOS NO PORTAL BASE COMO RELACIONADOS COM CIBERSEGURANÇA



Fonte: CNCS

A certificação da cibersegurança tem como principal propósito atestar a conformidade de uma entidade, serviços, processo ou produto, com determinados requisitos de cibersegurança, através da aplicação de uma metodologia de avaliação reconhecida pelas entidades competentes para o efeito, envolvendo frequentemente auditorias e análises documentais por parte de entidades externas. Por envolver uma avaliação externa com base em metodologias reconhecidas, os certificados de cibersegurança atribuídos às organizações oferecem-nos um importante indicador indireto do estado da capacitação das organizações em Portugal.

23 Dados disponíveis no Plataforma aberta de dados públicos portugueses: https://dados.gov.pt/pt/datasets/contratos-publicos-portal-base-impic-contratos-de-2012-a-2025/

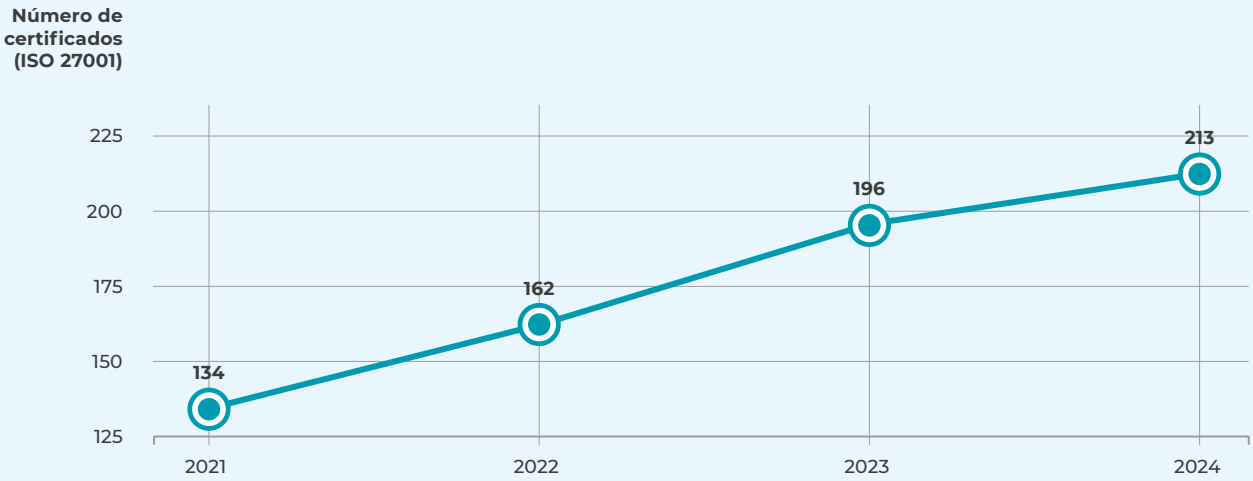
24 Por exemplo, expressões relacionadas com normas de cibersegurança, sistemas de autenticação, sistemas de deteção de intrusões, segurança das redes, testes de penetração e auditorias, resposta a incidentes, *threat intelligence*, criptografia e proteção de dados etc.

O Selo de Maturidade Digital – Cibersegurança atesta a adoção de uma série de requisitos técnicos relacionados com a cibersegurança[25]. Estes requisitos organizados em três níveis de maturidade Bronze, Prata ou Ouro, consoante o grau de exigência técnica de cada um. Em novembro de 2025, 22 entidades, públicas e privadas, tinham sido certificadas: 8 entidades com selo Ouro, 9 entidades com o selo Prata e 5 entidades com selo Bronze.

A ISO/IEC 27001 é, por sua vez, uma norma internacional de referência que especifica os requisitos técnicos para implementar e manter continuamente um sistema de gestão da informação. Com base em dados recolhidos da base nacional de empresas certificadas do Instituto Português de Acreditação (IPAC)[26], analisamos, abaixo, o número de entidades certificadas com esta norma entre 2021 e 2024. Os dados sugerem um crescimento sustentado e quase linear, pelo menos desde 2021. Em 2024, pelo menos 213 entidades estavam certificadas para a norma 27001, o que representa um aumento de 72% desde 2021.

Figura 62

NÚMERO DE EMPRESAS CERTIFICADAS COM A NORMA ISO/IEC 27001



Fonte: IPAC

SENSIBILIZAÇÃO

As ações de sensibilização variam no seu público-alvo, assim como no tipo de conteúdo e formato de disseminação. Comum a todas estas ações é o objetivo de consciencializar um determinado público para os efeitos nefastos dos riscos das ciberameaças e vulnerabilidades existentes, levando esse público a adotar comportamentos mais seguros na interação com as TIC. As tipologias mais frequentes das ações de sensibilização são os cursos de *e-learning*, os chamados MOOC (acrónimo do inglês *Massive Open Online Course*, em português Curso em linha aberto e massivo), as campanhas de sensibilização e a produção e difusão de boas práticas de ciber-higiene. Convém relembrar, no entanto, que o comportamento mais ou menos seguro na utilização das TIC não depende apenas do conhecimento das pessoas relativamente à cibersegurança ou tecnologias disponíveis, havendo outros fatores internos (p. ex. nível de educação, domínio linguístico) e externos (p. ex. enquadramento organizacional, existência ou não de sanções por incumprimento de práticas, stress no trabalho) que podem ter impacto nesses comportamentos e, por sua vez, na cibersegurança das organizações (Chowdhury et al, 2019; McCormac et al., 2018).

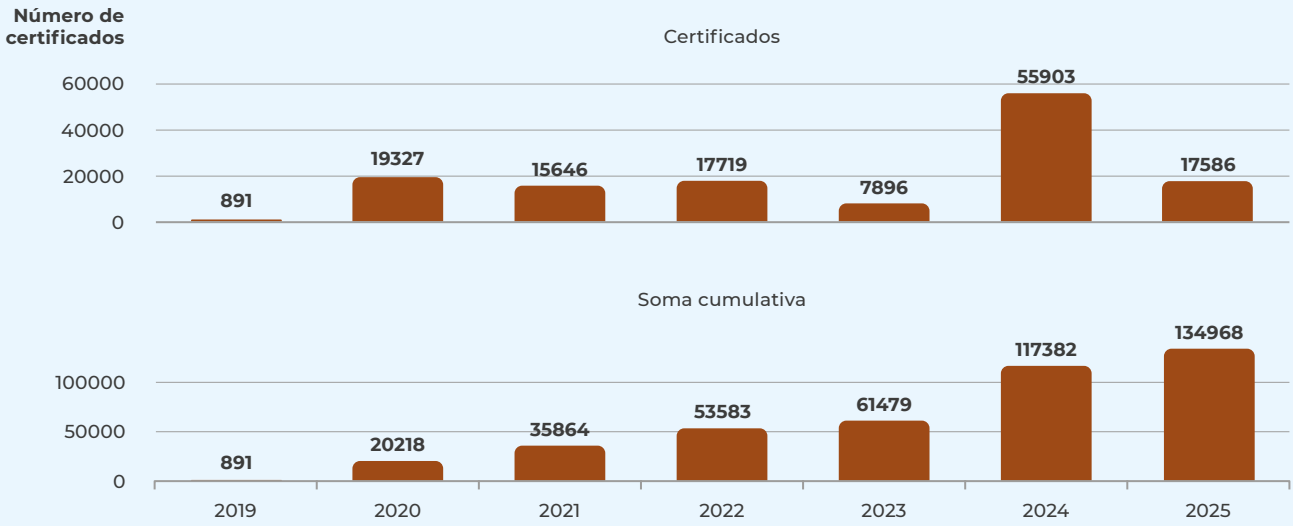
25 https://selosmaturidadedigital.incm.pt/Cybersecurity
26 http://www.ipac.pt/pesquisa/bdec2.html

A análise abaixo foca-se no recurso aos cursos de *e-learning* como ferramenta de sensibilização para a ciber-higiene. A ênfase atribuída a esta tipologia deve-se, por um lado, ao facto de existir evidência em vários domínios que sugere que atividades de sensibilização pro-ativas como os MOOCs, ou atividades de *gamificação*, tendem a ser eficazes na consciencialização de certos fenómenos específicos (Ferrari et al., 2019; Roozenbeek & Van der Linden, 2019). Por outro, estes cursos tendem a ter momentos de avaliação que, ainda que possam variar na sua forma e grau de exigência, nos permite obter um indicador para o seu impacto. Algo mais difícil no caso de campanhas de sensibilização de outra natureza (van Steen, 2020).

Para esta análise, recolheram-se dados relativos a todos os cursos relacionados com a sensibilização para boas práticas de ciber-higiene[27] presentes na plataforma NAU[28]. Na nossa análise identificámos 105 cursos de *e-learning* deste tipo únicos oferecidos na plataforma NAU[29]. Analisando o número de certificados emitidos no âmbito destes cursos, verifica-se, ao longo do tempo[30], um crescimento substancial no número de certificados emitidos, passando de 891, em 2019, a 134,968, até à data de outubro de 2025. O primeiro grande salto foi dado em 2020 com um aumento de 18,436 no número de certificados emitidos em cursos que terminaram neste ano relativamente aos cursos que terminaram no ano anterior. O segundo grande momento dá-se em 2024, com a emissão de 55,903 certificados em cursos que terminaram neste ano, o que representa um aumento de aproximadamente 608% relativamente aos 7,896 do ano anterior.

Figura 63

NÚMERO DE CERTIFICADOS (E SOMA CUMULATIVA) EMITIDOS EM CURSOS SOBRE CIBERHIGIENE E BOAS PRÁTICAS DE CIBERSEGURANÇA



Fonte: NAU/CNCS

A sensibilização também pode ocorrer num contexto institucional, nomeadamente através de ações de sensibilização ou formações de ciber-higiene em empresas e organismos da administração pública. Segundo dados de um inquérito do Eurobarómetro (2024), de maio de 2024, aproximadamente 26% das empresas portuguesas considerava ter disponibilizado ações de sensibilização ou formações sobre cibersegurança nos últimos 12 meses. Este valor é bastante próximo do da média da UE (25%), sendo a Chéquia e a Alemanha os países onde esta percentagem é mais elevada, chegando aos 41%, sendo mais baixa em França e na Roménia, com cerca de 9% das empresas. Por outro lado, a percentagem relativa de empresas em Portugal,

27 Para ser considerado um curso de ciber-higiene, o curso deveria i) ter este como o tema central do seu conteúdo e ii) ser dirigido ao público em geral e não apenas para substratos da população ou para a capacitação técnica de indivíduos nas áreas das TIC ou cibersegurança.

28 https://www.nau.edu.pt/pt/.

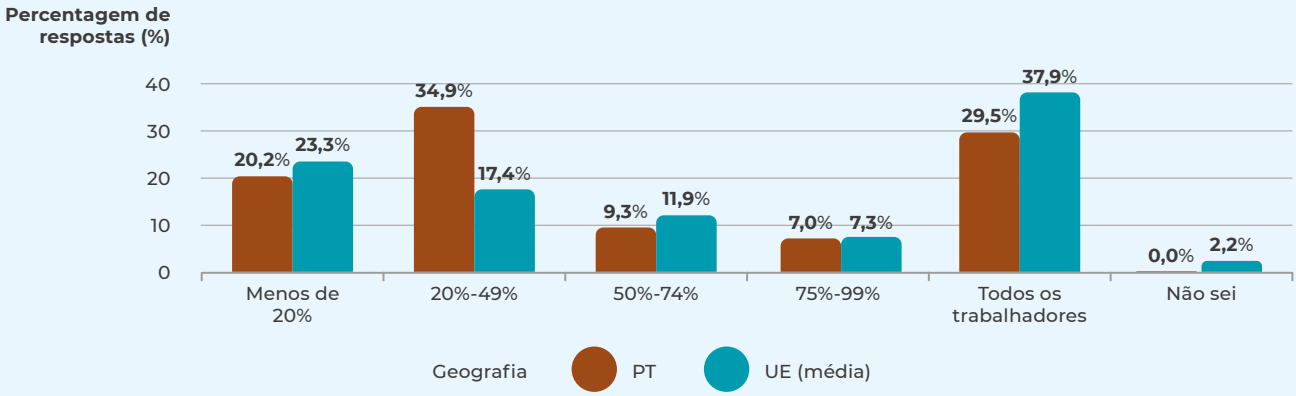
29 Note-se que um curso pode ter mais do que uma edição.

30 Para quantificar o número de certificados, considerou-se o ano de fecho do curso como ponto de referência.

em 2024, nas quais todos os trabalhadores participaram em ações de sensibilização ou de formação de cibersegurança, nos últimos 12 meses, é de aproximadamente 29%, valor 8 pp abaixo da média europeia. Aproximadamente 1 em cada 3 empresas portuguesas considera que entre 20% e 49% dos seus trabalhadores receberam ações de sensibilização ou formações de cibersegurança.

Figura 64

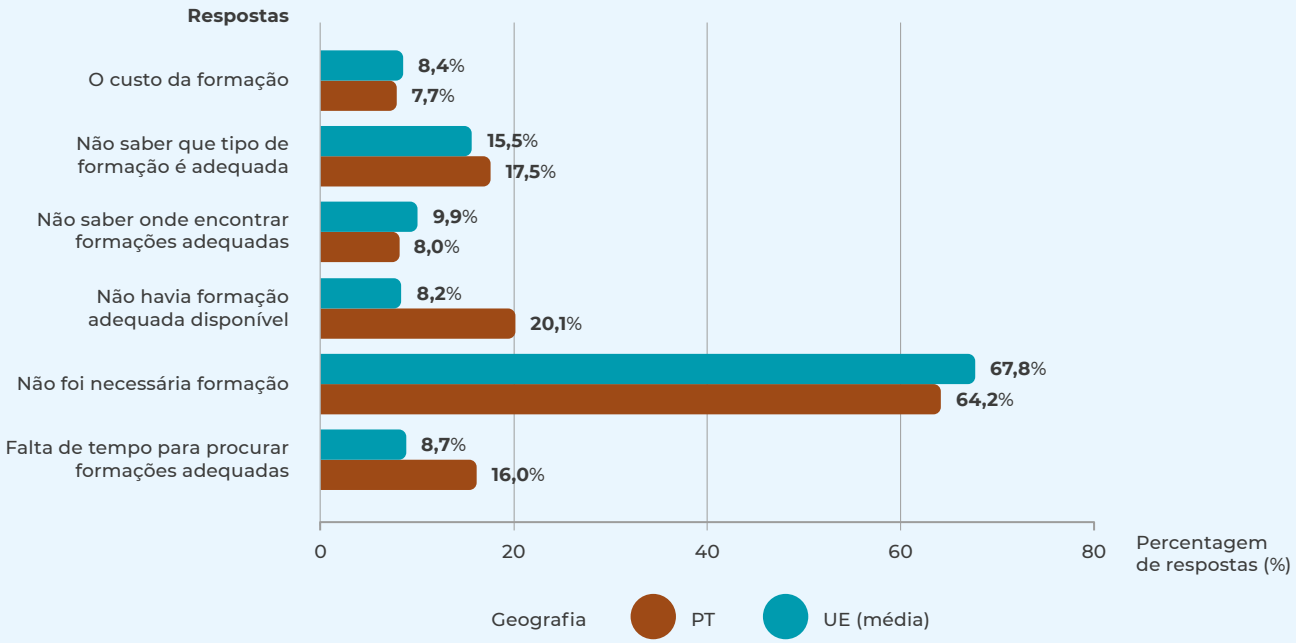
PERCENTAGEM DE TRABALHADORES QUE PARTICIPARAM EM AÇÕES DE SENSIBILIZAÇÃO SOBRE CIBERSEGURANÇA



Fonte: Eurobarómetro

Figura 65

MOTIVOS PARA NÃO OFERECER AÇÕES DE SENSIBILIZAÇÃO AOS TRABALHADORES



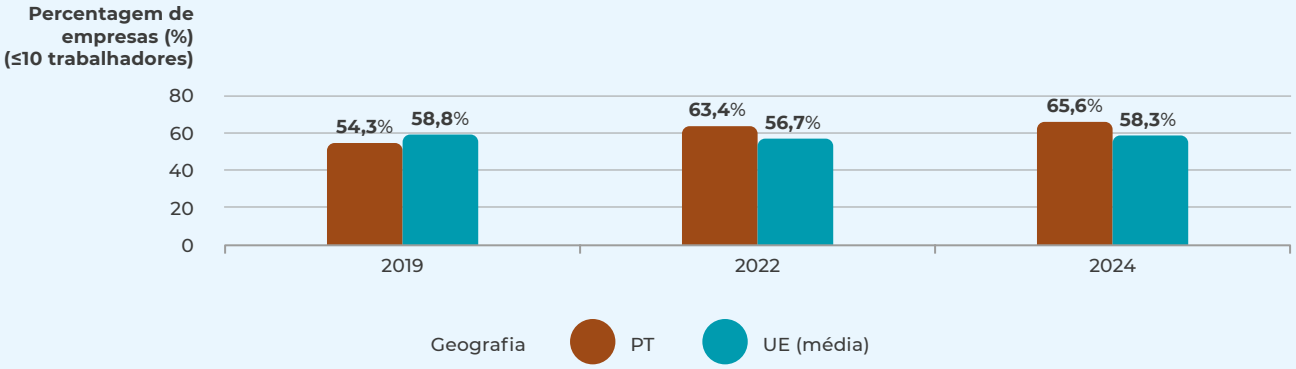
Fonte: Eurobarómetro

Tal como a maioria dos Estados-Membros, a maioria das empresas portuguesas inquiridas que responderam não ter oferecido ações de sensibilização ou formações de cibersegurança aos seus trabalhadores, não o fizeram por considerarem desnecessário (aproximadamente 64%). Cerca de 20% das empresas portuguesas responderam que não foram disponibilizadas ações de sensibilização ou formações por falta de oferta formativa adequada disponível no mercado, valor acima da média da UE (8%). O resto das respostas é bastante residual, sendo considerado por uma em cada 6 empresas. O custo, um fator frequentemente discutido, parece ter sido o motivo menos relevante, tendo sido apenas considerado por 7% das empresas portuguesas, valor semelhante ao da média da UE.

Recorremos também a dados do Eurostat para analisar os métodos de sensibilização adotados pelas empresas junto dos seus funcionários. Em Portugal, a percentagem de empresas que promoveram ações de sensibilização aumentou significativamente desde 2019, quando se situava nos 54,3%, até 2024, ano em que aproximadamente duas em cada três empresas afirmaram ter realizado iniciativas de sensibilização para a cibersegurança (Eurostat, 2024gj). Esta evolução contrasta com a trajetória da UE, cuja média se manteve relativamente estável entre 58% e 59% no período de 2019 a 2024.

Figura 66

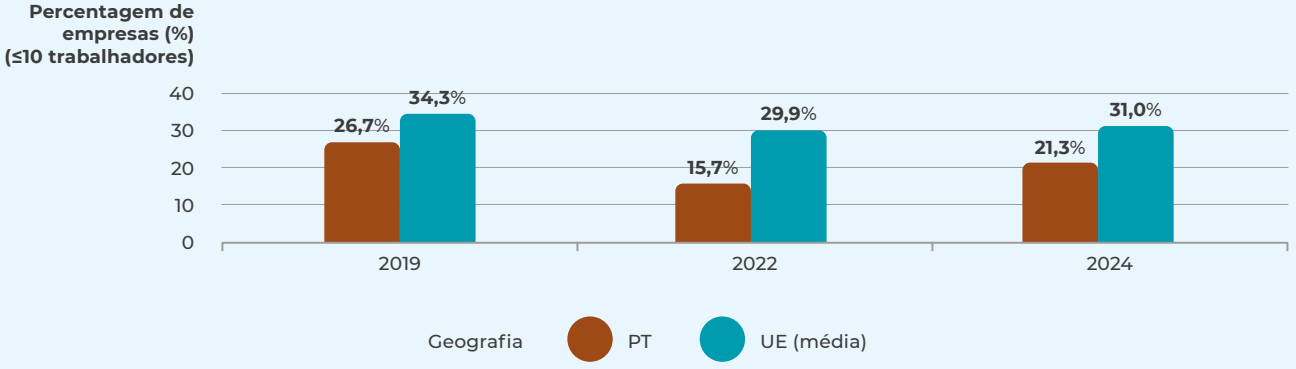
PERCENTAGEM DE EMPRESAS QUE SENSIBILIZARAM OS SEUS TRABALHADORES PARA A CIBERSEGURANÇA



Fonte: Eurostat

Figura 67

PERCENTAGEM DE EMPRESAS QUE SENSIBILIZARAM OS SEUS TRABALHADORES PARA A CIBERSEGURANÇA ATRAVÉS DE DISPOSIÇÕES CONTRATUAIS



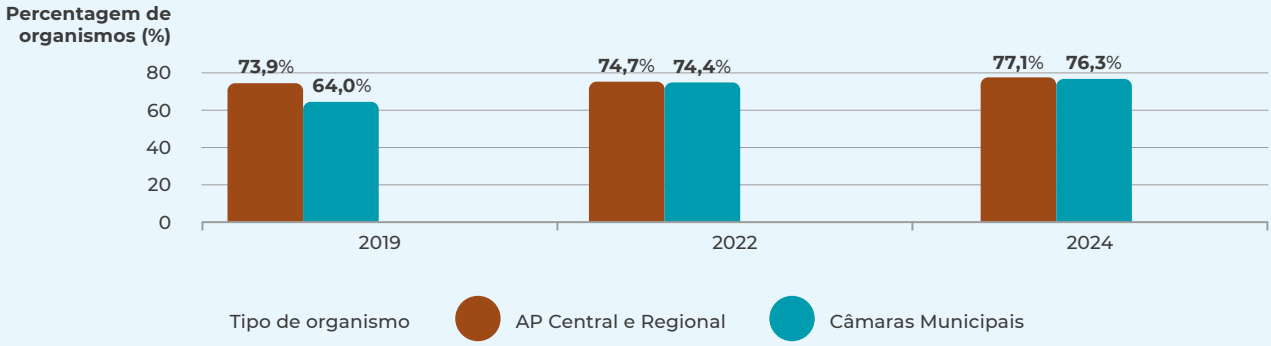
Fonte: Eurostat

Além disso, enquanto a média da UE privilegia métodos de caráter compulsivo, como formações obrigatórias (23,8% em 2024) ou disposições contratuais (31% em 2024), as empresas portuguesas tendem a optar por formações de natureza voluntária. Em 2024, 55% recorreram a documentos internos de sensibilização, em comparação com 21,2% que realizaram formações obrigatórias e 21,3% que recorreram a disposições contratuais.

À semelhança do que se observa nas empresas, os organismos da administração pública têm vindo a investir em ações de sensibilização junto dos seus trabalhadores. As formações voluntárias e a disponibilização de documentação interna continuam a ser, de longe, os métodos mais utilizados com respetivamente cerca de 77,1% dos organismos da administração pública central/regional e 76,3% das câmaras municipais recorrem a estas práticas. Este valor manteve-se relativamente estável no caso da administração pública central/regional, contudo aumentou 12,3 pp de 2022 para 2024.

Figura 68

PERCENTAGEM DE ORGANISMOS DA AP QUE SENSIBILIZARAM OS SEUS TRABALHADORES PARA A CIBERSEGURANÇA ATRAVÉS DE AÇÕES DE FORMAÇÃO VOLUNTÁRIAS OU DOCUMENTAÇÃO INTERNA

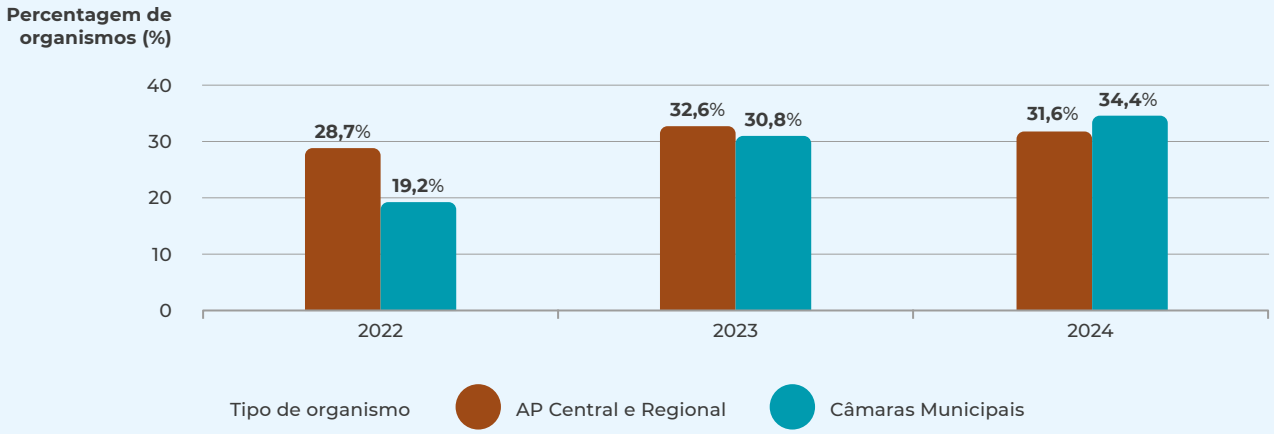


Fonte: Eurostat

Em 2024, cerca de dois em cada três organismos municipais recorreram a disposições contratuais para garantir a sensibilização para a cibersegurança, valor que aumentou 10 pp desde 2022. Nos organismos da administração pública central/regional, a percentagem atingiu 37,6% em 2024, registando uma subida mais moderada face aos 31,5% de 2022. Verifica-se também um aumento substancial no recurso a formações obrigatórias nos organismos municipais na ordem dos 15 pp desde 2022, alcançando 34,4% em 2024. Já na administração pública central/regional, o valor situou-se nos 31,6% e manteve-se relativamente estável ao longo do período observado.

Figura 69

PERCENTAGEM DE ORGANISMOS DA AP QUE SENSIBILIZARAM OS SEUS TRABALHADORES PARA A CIBER-SEGURANÇA ATRAVÉS DE AÇÕES DE FORMAÇÃO OBRIGATÓRIAS



Fonte: DGEEC

EDUCAÇÃO

CIBERSEGURANÇA NO ENSINO SUPERIOR

As empresas e entidades públicas, como vimos acima, consideram não existir profissionais em quantidade suficiente para suprir as necessidades crescentes na área de cibersegurança. Conscientes deste problema, as instituições de ensino superior têm vindo a aumentar o peso da cibersegurança nos seus cursos e disciplinas.

Abaixo analisamos a presença da cibersegurança no ensino superior. Com base em dados da Direção-Geral do Ensino Superior[31] e da Agência de Avaliação e Acreditação do Ensino Superior, analisamos, primeiro, o número de cursos acreditados, dos graus de licenciatura ao doutoramento, sobre cibersegurança ou segurança da informação, com base em dados recolhidos em outubro de 2025. Constata-se a existência de um número muito reduzido de cursos especializados ao nível das licenciaturas e doutoramentos em Portugal, tanto no ensino superior público como privado. Existe, por um lado, uma maior oferta do lado dos cursos técnicos superiores profissionais (120 créditos) ministrados no ensino politécnico que, apesar de serem cursos de ensino superior, não conferem grau académico, mas atribuem um diploma que permite o acesso aos ciclos de estudos de licenciatura e integrados de mestrado através de concursos especiais[32]. Por outro lado, ao nível dos cursos conferentes de grau académico superior, existe uma maior aposta na criação de ciclos de estudos de mestrado especializados em cibersegurança ou segurança da informação no ensino público.

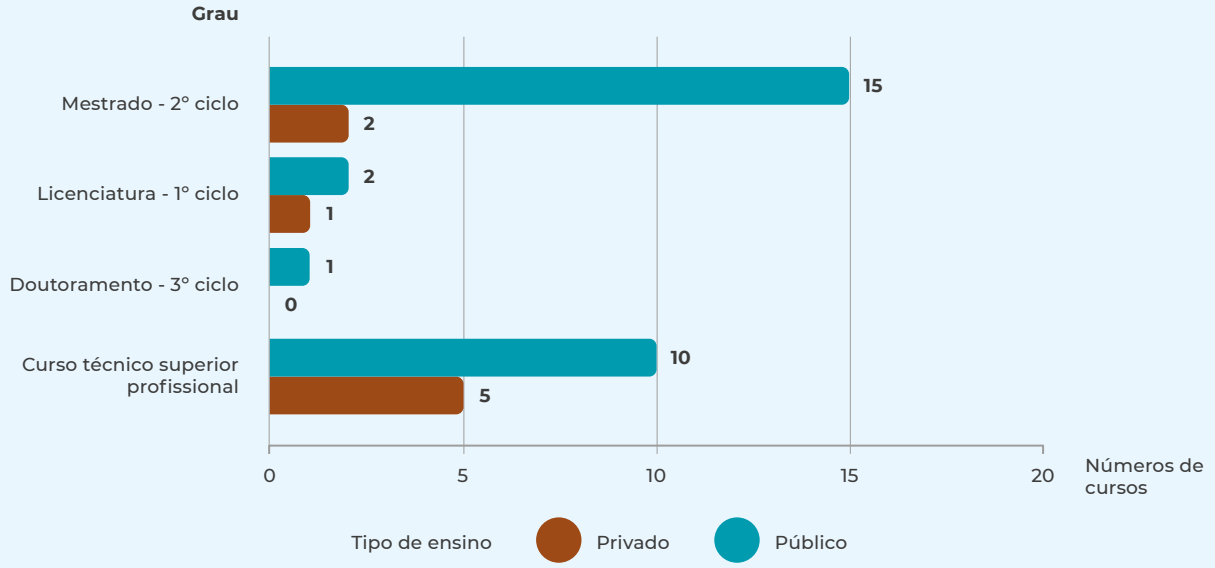
Contudo, outros cursos de ensino superior relativos às TIC podem ser a porta de entrada para a cibersegurança. Abaixo analisados dados sobre a presença de disciplinas de cibersegurança, obrigatórias ou opcionais, em 116 licenciaturas de TIC. Destas cerca de 47% não tinham qualquer disciplina de cibersegurança obrigatória e outros 47% tinham uma disciplina obrigatória, 4 cursos tinham 2 disciplinas obrigatórias e 2 cursos chegam mesmo a ter 3 disciplinas. O retrato muda ligeiramente quando consideramos também as disciplinas opcionais de cibersegurança. Apenas 36% dos cursos de TIC não têm nem disciplinas obrigatórias nem opcionais relacionadas com cibersegurança. Cerca de metade das licenciaturas consideradas têm uma disciplina de cibersegurança, enquanto 11% chegam mesmo a ter duas e aproximadamente 3% dos cursos têm 3 disciplinas de cibersegurança.

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

32 Decreto-Lei n.º 74/2006, de 24 de março, na sua versão atual.

Figura 70

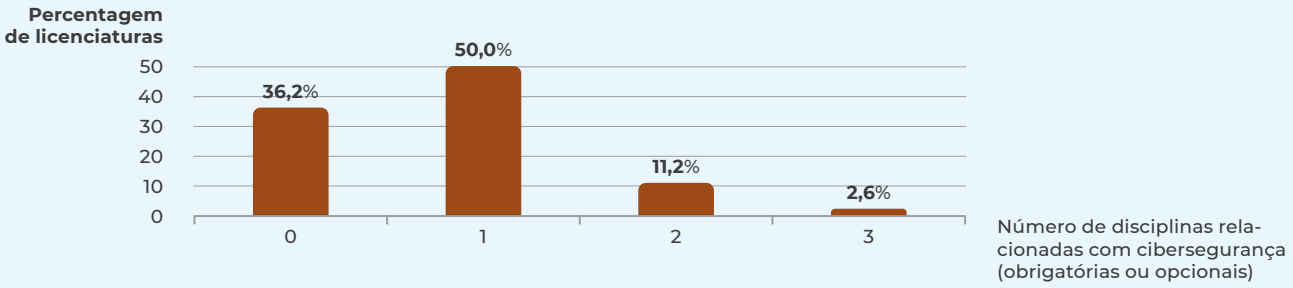
NÚMERO DE CURSOS UNIVERSITÁRIOS DE CIBERSEGURANÇA OU SEGURANÇA DA INFORMAÇÃO



Fonte: DGES/A3ES

Figura 71

PERCENTAGEM DE CURSOS DAS TIC POR NÚMERO DE DISCIPLINAS DE CIBERSEGURANÇA (OPCIONAIS OU OBRIGATÓRIAS)



Fonte: DGEEC

O número de alunos inscritos em cursos superiores relacionados com a cibersegurança continua a aumentar de forma sustentada. No ano letivo 2024/2025, registaram-se 1548 inscrições em cursos neste domínio, o que representa um crescimento de 7% face ao ano anterior. Deste total, apenas cerca de 8% correspondem a estudantes do sexo feminino, o mesmo valor observado no ano letivo anterior.

F. NOTAS METODOLÓGICAS

O presente documento foi desenvolvido com base em vários tipos de dados. Enquanto algumas estatísticas e métricas foram produzidas por entidades externas ao CNCS, outras foram produzidas pelo CNCS com base em dados brutos disponibilizados por outras entidades ou recolhidos de fontes abertas.

Os números sobre a exposição ao digital, bem como os relativos à privacidade e proteção dos dados pessoais ou às competências digitais, foram desenvolvidos pelo Eurostat com base no inquérito *Survey on the use of ICT in households and by individuals*[33]. O Instituto Nacional de Estatística (INE, 2024a) é o responsável pela sua recolha em Portugal. A recolha de dados para este inquérito decorreu de 16 de maio a 25 de agosto de 2024 e as estatísticas apresentadas foram estimadas com base numa amostra de 8 547 agregados domésticos com pelo menos uma pessoa com idade dos 16 aos 74 anos.

No que se refere a métricas relativas a empresas, nomeadamente a sua exposição ao digital ou medidas organizativas, uma parte substancial das estatísticas apresentadas tem origem no inquérito *ICT usage in enterprises*[34], também este administrado pelo INE (2024b). Este inquérito tem como população-alvo as empresas não financeiras ativas, sob a forma jurídica de sociedade, com sede em Portugal, com atividade principal classificada nas secções C, D, E, F, G, H, I, J, L, M, N e grupo 951 da secção S da Classificação Portuguesa de Atividades Económicas, Revisão 3 (CAE Rev. 3). Consideraram-se apenas empresas com 10 ou mais trabalhadores. O período de resposta ao inquérito decorreu entre fevereiro e junho de 2024, resultando numa amostra de 8 436 respostas válidas ao inquérito.

Ainda neste âmbito, a componente referente às competências em cibersegurança nas empresas foi desenvolvida a partir do inquérito do Eurobarómetro feito no âmbito do *Flash Eurobarometer 547 Cyberskills*, o qual foi aplicado entre abril e maio de 2024, tendo sido conduzidas nesse período 503 entrevistas a empresas em Portugal (Eurobarometer, 2024).

As métricas relacionadas com a exposição à desinformação foram recolhidas do inquérito do Eurobarómetro *Social Media Survey 2025 | FL014EP*. O trabalho de campo ocorreu entre 11 e 18 de junho 2025, tendo sido atingida uma amostra de 1 018 indivíduos em Portugal (Eurobarometer, 2025a).

Os dados sobre a administração pública são recolhidos anualmente pela DGEEC nos dois Inquéritos à Utilização das TIC, um dirigido à administração pública central e regional e o outro às câmaras municipais, realizados entre outubro de 2024 a março de 2025, obtendo-se as respostas de 367 organismos da administração pública central e regional e de 308 câmaras municipais.

33 Para mais detalhe consultar as seguintes páginas: https://ec.europa.eu/eurostat/cache/metadata/EN/isoc_i_simsih2_pt.htm

34 Para mais detalhe consultar as seguintes páginas: https://ec.europa.eu/eurostat/cache/metadata/EN/isoc_e_simsie_pt.htm

Para analisar a saliência da cibersegurança na sociedade portuguesa, recorreu-se a dois tipos de dados: a cobertura mediática do tema e incidência do tema nas pesquisas *online* dos portugueses. A análise da cobertura mediática foi feita com base em dados recolhidos da plataforma *Media Cloud*[35] (Robert et al., 2021). Utilizando uma lista de palavras-chave relacionadas com a cibersegurança, contou-se o número de artigos por dia com base numa lista de 89 meios de comunicação[36]. Para os dados relativos às pesquisas em motores de busca recorreu-se à plataforma *Google Trends*[37] que fornece dados que medem o volume relativo das pesquisas no motor de busca Google associado a um termo, normalizado pelo valor total das pesquisas numa certa geografia e num determinado intervalo de tempo[38]. O resultado é um índice de 0 a 100 que aproxima a popularidade relativa de um certo termo de pesquisa relativamente a outros pesquisados em contexto semelhante.

A informação apresentada sobre o número de cursos de cibersegurança e segurança da informação, bem como alunos inscritos e diplomados nos mesmos, foi recolhida no *website* da Direção-Geral do Ensino Superior (DGES), no motor de pesquisa de cursos, utilizando-se para o efeito as palavras-chave "cibersegurança" e "segurança", tendo sido depois validado cada curso[39]. Este procedimento foi replicado na base de dados da Agência de Avaliação e Acreditação do Ensino Superior (A3ES)[40]. Relativamente ao número de alunos inscritos, a informação foi recolhida no *website* da DGEEC, utilizando-se as mesmas palavras-chave. Para o levantamento do número de disciplinas relacionadas com a cibersegurança, analisaram-se os programas curriculares de uma amostra de 116 licenciaturas das TIC de instituições presentes em todos os distritos de Portugal e regiões autónomas.

Os dados relativos a MOOCs relacionados com ciber-higiene ou cibersegurança foram recolhidos da plataforma NAU[41]. Para esta análise, considerámos 126 cursos.

O investimento económico por parte das organizações foi mensurado com base em duas fontes de dados. Primeiro, analisou-se os investimentos económicos na cibersegurança por parte de entidades nos setores cobertos pela diretiva NIS2 com recurso aos dados recolhidos pela ENISA no seu inquérito anual para o relatório *NIS Investments* (ENISA, 2024). Este inquérito foi administrado a uma amostra de 1350 organizações da união europeia, cerca de 50 por Estado-membro. Para aproximar os valores dos investimentos em cibersegurança por parte da administração pública, criou-se um *dataset* original com informação relativa a contratos públicos presentes no portal base[42] relacionados com tecnologias ou serviços tradicionalmente associados à cibersegurança. Os dados foram compilados da seguinte forma: primeiro recolheu-se informação relativa a todos os contratos públicos celebrados entre 2013 e 2024, utilizando para o efeito os acima mencionados dados do portal base; em seguida, filtraram-se os contratos públicos em que a descrição do objeto contratual correspondia a expressões regulares relacionadas com tecnologias ou serviços de cibersegurança. Na escolha das palavras-chave relevantes privilegiou-se palavras-chave que minimizavam a probabilidade de falsos-positivos (e.g. evitar certas siglas como MFA), o que, em muitas instâncias, implica um ligeiro aumento nos falsos-negativos. Os resultados devem, por isso, ser interpretados como um limite inferior, ou estimativa conservadora, do número real de contratos.

As estatísticas produzidas relativamente a certificações de cibersegurança recorreram á base de dados nacional de empresas certificadas do Instituto Português de Acreditação (IPAC), nomeadamente relativamente ao número de entidades certificadas com a norma ISO-27001.

35 Para mais detalhe, ver: www.mediacloud.org/documentation/search-tool-guide.
36 https://search.mediacloud.org/collections/34412337.
37 https://trends.google.com/trends/.
38 https://support.google.com/trends/answer/4365533?hl=en.
39 https://www.dges.gov.pt/simges/public/www/cursos_instituicoes?plid=372 e https://www.dgeec.medu.pt/p/ensino-superior
40 https://a3es.pt/pt/avaliacao-e-acreditacao/resultados-dos-processo-de-avaliacao-e-acreditacao/acreditacao-de-ciclos-de-estudos/
41 https://www.nau.edu.pt/pt/cursos/?limit=21&offset=0
42 https://dados.gov.pt/pt/datasets/contratos-publicos-portal-base-impic-contratos-de-2012-a-2025/

Para analisar a incidência relativa de vulnerabilidades recorreu-se aos dados de fonte aberta da fundação *Shadow Server*[43]. De forma a se conseguir fazer uma análise comparada recorreu-se, para cada país e dado um conjunto de 148 vulnerabilidades[44] em análise, à seguinte técnica de agregação:

1. Para cada país, calculou-se o número mediano de endereços de IPs vulneráveis por milhão de habitantes relativamente a todos os CVEs. Primeiro, para cada CVE, calculou-se o rácio entre o número de endereços de IPs vulneráveis nesse país e a sua população (em milhões), o que nos dá uma medida de endereços de IPs vulneráveis *per capita*. Em seguida calculou-se o valor mediano, relativamente ao país como um todo, como método de agregação. A escolha deste método de agregação em vez de outros, como a média, deve-se ao facto de existirem muitos valores extremos (*outliers*). Assim, ficamos com o número mediano de IPs vulneráveis *per capita*.
2. Os países foram depois ordenados de acordo com o número mediano de endereços de IPs vulneráveis *per capita*, calculados no passo anterior, ficando ordenados do país com o menor valor mediano, que recebe o ranking de 1, ao país com o maior número mediano de vulnerabilidades per capita, que recebe o ranking de N. Neste caso, como se procurou comparar Portugal com os restantes Estados-membros, N=27.
3. Por último, normalizou-se o ranking de cada país dividindo-o pelo número total de países, N=27, de forma a conseguir produzir um valor normalizado entre 0 e 1.

A informação relativa à exploração das vulnerabilidades em campanhas de *ransomware* foi recolhida da base de dados KEV da CISA[45].

Os dados sobre o estado da implementação de *standards* da internet e de *email* têm duas fontes. A primeira fonte é a base de dados relativos ao projeto *Key Internet Standards Deployment Monitoring* (KISDM), desenvolvido pelo *Directorate General for Communications Networks, Content and Technology* e do *Joint Research Centre* da Comissão Europeia, que recorre a dados públicos ou a scanners concebidos para o efeito, com o objetivo de avaliar a adoção de normas cruciais para as comunicações seguras (DG CONNECT & JRC, 2025). Desde o terceiro trimestre de 2023, os dados são calculados com base em scanners que analisam sites da lista Tranco[46] (Pochat et al., 2018), devendo ser interpretados como a percentagem de páginas que adotam a norma[47]. Esta métrica deve ser entendida como um método de recolha exaustivo, próximo de um censo da internet. A segunda fonte de dados frequentemente utilizada são os dados do Observatório de Tecnologias da Internet Portuguesa, pertencente ao capítulo português da *Internet Society Foundation* (ISOC-PT)[48]. Ao contrário da análise do projeto KISDM, que mostra proporções relativas ao equivalente da população relevante da internet, os dados do ISOC-PT analisam a implementação de normas relevantes para as comunicações seguras e para a cibersegurança por parte de sites sociologicamente relevantes, tais como páginas de organismos públicos, órgãos de comunicação social ou páginas de empresas do PSI-20. A instrumentação utilizada nesta análise recorre, em parte, ao *software* de código aberto do projeto Internet.nl[49]. Para esclarecimento de dúvidas adicionais sobre as metodologias adotadas, contactar o CNCS através do seguinte *email*: observatorio@cncs.gov.pt.

43 https://www.shadowserver.org/.

44 Cve-2017-6736, cve-2018-19410, cve-2019-0708, cve-2019-5544, cve-2020-0688, cve-2020-3992, cve-2021-21972, cve-2021-21974, cve-2021-26855, cve-2021-27065, cve-2021-35587, cve-2022-24816, cve-2022-26143, cve-2022-27510, cve-2022-37042, cve-2022-41082, cve-2022-42475, cve-2023-20892, cve-2023-21529, cve-2023-22515, cve-2023-23752, cve-2023-25157, cve-2023-2533, cve-2023-25690, cve-2023-27350, cve-2023-27997, cve-2023-33157, cve-2023-33160, cve-2023-33308, cve-2023-34048, cve-2023-35078, cve-2023-35082, cve-2023-3519, cve-2023-36439, cve-2023-36745, cve-2023-38646, cve-2023-39143, cve-2023-39335, cve-2023-42793, cve-2023-43177, cve-2023-43208, cve-2023-43261, cve-2023-45590, cve-2023-46747, cve-2023-48365, cve-2023-48788, cve-2023-48795, cve-2023-49103, cve-2023-49606, cve-2023-4966, cve-2023-6549, cve-2023-7028, cve-2024-0012, cve-2024-0204, cve-2024-10443, cve-2024-11680, cve-2024-1709, cve-2024-20419, cve-2024-21410, cve-2024-21762, cve-2024-21894, cve-2024-22024, cve-2024-22053, cve-2024-22252, cve-2024-23692, cve-2024-23897, cve-2024-23917, cve-2024-26198, cve-2024-27198, cve-2024-28986, cve-2024-28987, cve-2024-28995, cve-2024-3273, cve-2024-3400, cve-2024-36401, cve-2024-37079, cve-2024-37085, cve-2024-38018, cve-2024-38094, cve-2024-38812, cve-2024-4040, cve-2024-42448, cve-2024-4358, cve-2024-45186, cve-2024-45519, cve-2024-45711, cve-2024-48248, cve-2024-48887, cve-2024-50623, cve-2024-52875, cve-2024-55579, cve-2024-55591, cve-2024-55956, cve-2024-57727, cve-2024-6235, cve-2024-6327, cve-2024-7399, cve-2025-0282, cve-2025-0994, cve-2025-10035, cve-2025-11371, cve-2025-20333, cve-2025-20362, cve-2025-20363, cve-2025-21400, cve-2025-22224, cve-2025-22457, cve-2025-22467, cve-2025-24801, cve-2025-26399, cve-2025-26793, cve-2025-2775, cve-2025-2825, cve-2025-29794, cve-2025-30406, cve-2025-31161, cve-2025-31324, cve-2025-32433, cve-2025-34158, cve-2025-3935, cve-2025-40596, cve-2025-40778, cve-2025-41236, cve-2025-41237, cve-2025-41238, cve-2025-42944, cve-2025-43928, cve-2025-4427, cve-2025-4632, cve-2025-47163, cve-2025-47812, cve-2025-48827, cve-2025-49701, cve-2025-49706, cve-2025-53770, cve-2025-53786, cve-2025-54309, cve-2025-54451, cve-2025-55145, cve-2025-5777, cve-2025-57819, cve-2025-61882, cve-2025-62763, cve-2025-6543, cve-2025-7775, cve-2025-8875, cve-2025-8876 e cve-2025-9242.

45 https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

46 https://tranco-list.eu/

47 https://ec.europa.eu/internet-standards/methodology.html.

48 https://observatory.isoc.pt/docs.html

49 https://internet.nl/

G. REFERÊNCIAS PRINCIPAIS

RELATÓRIOS

[consultados a 13/02/2026]

- CNCS (2025) Relatório Cibersegurança em Portugal – Riscos & Conflitos 2025. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/rel-riscosconflitos2025-obcibercncs.pdf
- CNCS (2023) *Relatório Cibersegurança em Portugal – Sociedade 2023*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/rel-sociedade2023-observ-cncs-dig.pdf
- ENISA (2025) *ENISA Threat Landscape 2025*. ENISA-European Union Agency for Cybersecurity. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
- ENISA (2024) *NIS Investments – Cybersecurity Policy Assessment*. ENISA-European Union Agency for Cybersecurity. Disponível em: https://www.enisa.europa.eu/publications/nis-investments-2024
- NIS Cooperation Group (2023) *Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies*. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group
- OECD. (2021) *Encouraging Vulnerability Treatment: Overview for policy makers*, OECD Digital Economy Papers, no. 307. Disponível em: https://www.oecd.org/en/publications/encouraging-vulnerability-treatment_0e2615ba-en.html
- Kouliaridis, V., Kounelis, I. (2025a) *Internet Standards: Web communication standards - an analysis of uptake in the EU*. Publications Office of the European Union. Disponível em: https://data.europa.eu/doi/10.2760/5587977
- Kouliaridis, V., Kounelis, I. (2025b) *Internet Standards: Email communication security standards - an analysis of uptake in the EU*. Publications Office of the European Union. Disponível em: https://data.europa.eu/doi/10.2760/5576432, JRC143105
- UNESCO Institute for Statistics (2018) *A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2*. UIS/2018/ICT/IP/51. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000265403.locale=en

INQUÉRITOS

[consultados a 19/11/2025]

- DGEEC (2024a) *Inquérito à Utilização das Tecnologias da Informação e Comunicação na Administração Pública Central e Regional – IUTICAP 2024*. Direção-Geral de Estatísticas da Educação e Ciência. Disponível em: https://www.dgeec.medu.pt/art/ciencia-e-tecnologia/undefined/undefined/666c30bbd8d9c90163a3f015
- DGEEC (2024b) *Inquérito à Utilização das Tecnologias da Informação e Comunicação nas Câmaras Municipais- IUTICCM 2024*. Direção-Geral de Estatísticas da Educação e Ciência. Disponível em: https://www.dgeec.medu.pt/art/ciencia-e-tecnologia/undefined/undefined/666c30d41638429280fe5991

- Eurostat (2024a) *ICT usage in enterprises, ICT security – Security incidents and consequences by size class of enterprise*. Eurostat. ISOC_CISCE_IC. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ic__custom_19004306/default/table
- Eurostat (2024b) *ICT usage in households and by individuals, Households - level of internet access*. Eurostat. ISOC_CI_IN_H. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_in_h$defaultview/default/table?lang=en
- Eurostat (2024c) *ICT usage in households and by individuals, Individuals - internet activities*. Eurostat. ISOC_CI_AC_I. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_ac_i__custom_19036786/default/table
- Eurostat (2024d) *ICT usage in enterprises, E-business – Cloud computing services by class of enterprise*. Eurostat. ISOC_CICCE_USE. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_cicce_use/default/table?lang=en&category=isoc.isoc_ e.isoc_eb
- Eurostat (2024e) *ICT usage in enterprises, Connection to the internet – Remote access by size class of enterprise*. Eurostat. ISOC_CICCE_USE. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_ras/default/table?lang=en&category=isoc.isoc_e.isoc_ci
- Eurostat (2024f) *ICT usage in enterprises, Artificial intelligence by size class of enterprise*. Eurostat. ISOC_EB_AI. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_eb_ai/default/table?lang=en
- Eurostat (2024g) *ICT security - Security policy, measures, risks and staff awareness by size class of enterprise*. Eurostat. ISOC_CISCE_RA. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ra/default/table?lang=en&category=isoc.isoc_e.isoc_cisc
- Eurostat (2024h) *ICT usage in households and by individuals, Internet of Things – barriers to use*. Eurostat. ISOC_IIOT_BX. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_iiot_bx/default/table?lang=en&category=degurb.degurb_isoc.du_isoc_i.du_isoc_iw
- Eurostat (2024i) *ICT usage in households and by individuals, E-government – Reasons for not submitting completed forms to public authorities' websites*. Eurostat. ISOC_CIEGI_RTX. Disponível: https://ec.europa.eu/eurostat/databrowser/view/isoc_ciegi_rtx/default/table?lang=en
- Eurostat (2023a) *Digital Skills, ICT users, Individuals' level of computer skills (2021 onwards)*. Eurostat. ISOC_SK_CSKL_I21. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_cskl_i21__custom_18914338/default/table
- Eurostat (2023b) *ICT usage in enterprises, Websites and use of social media*. Eurostat. ISOC_CIWEB. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_ciweb/default/table?lang=en&category=isoc.isoc_e.isoc_cism
- Eurostat (2023c) *ICT usage in households and by individuals, ICT trust, security and privacy - Privacy and protection of personal data. Eurostat*. ISOC_CISCI_PRV20. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_prv20__custom_18918642/default/table
- Eurostat (2023d) *Digital Skills. ICT users – Individual's level of digital skills*. Eurostat. ISOC_SK_DSKL_I21URL: https://ec.europa.eu/eurostat/databrowser/view/ISOC_SK_DSKL_I21/default/bar?lang=en&category=isoc.isoc_sk.isoc_sku
- Eurostat (2023e) *ICT usage in households and by individuals, E-government – Use of electronic identification (eID)*. Eurostat. ISOC_EID_IEID. Disponível em: https://ec.europa.eu/eurostat/databrowser/view/isoc_eid_ieid__custom_19064925/default/table
- Eurobarometer (2025a) *Flash Eurobarometer FL014EP: Social Media Survey 2025*. European Commision. Disponível em: http://data.europa.eu/88u/dataset/s3592_fl014ep_eng
- Eurobarometer (2025b) *Digital Decade 2025 - Special Eurobarometer*. European Commision. Disponível em: https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-special-eurobarometer
- Eurobarometer (2024) *Flash Eurobarometer FL547: Cyberskills*. European Commision. Disponível em: https://data.europa.eu/data/datasets/s3176_fl547_eng?locale=en

- DG CONNECT & JRC (2025) *EU Internet Standards Deployment Monitoring Website*. Directorate General for Communications Networks, Content and Technology, Joint Research Centre. European Commission. Disponível em: https://ec.europa.eu/internet-standards/index.html
- IMPIC (2024) *Contratos Públicos - Contratos de 2012 a 2026*. Instituto dos Mercados Públicos, do Imobiliário e da Construção. Portal Base. Disponível em: https://dados.gov.pt/pt/datasets/contratos-publicos-portal-base-impic-contratos-de-2012-a-2026/#/resources
- INE (2024a) *Sociedade da Informação e do Conhecimento - Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Famílias*. Instituto Nacional de Estatística. Disponível em: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=646170405&DESTAQUESmodo=2
- INE (2024b) *Sociedade da informação e do conhecimento Inquérito à utilização de tecnologias da informação e da comunicação nas empresas*. Instituto Nacional de Estatística. Disponível em: https://webinq.ine.pt/Public/DownloadFiles.aspx?idFile=5156

MONOGRAFIAS

[consultados a 13/02/2026]

- Alagheband, M. R., Mashatan, A., & Zihayat, M. (2020). Time-based gap analysis of cybersecurity trends in academic and digital media. *ACM Transactions on Management Information Systems, 11*(4). Disponível em: https://doi.org/10.1145/3389684
- Alsadi, A. A., et al. (2025). Bits and pieces: Piecing together factors of IoT vulnerability exploitation. *In Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. Association for Computing Machinery. Disponível em: https://doi.org/10.1145/3389684
- Chowdhury, N. H., Adam, M. T. P., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: A systematic literature review. *Behaviour & Information Technology, 38*(12). Disponível em: https://doi.org/10.1080/0144929X.2019.1583769
- Ferrari, E., et al. (2024). Improvement of attitudes and skills using a MOOC about the basic science of climate change. *Humanities and Social Sciences Communications, 11*(1). Disponível em: https://doi.org/10.1057/s41599-024-03139-6
- Herbert, F., Becker, S., Buckmann, A., Kowalewski, M., Hielscher, J., Acar, Y., Durmuth, M., Zou, Y., & Sasse, M. A. (2024). Digital security—A question of perspective: A large-scale telephone survey with four at-risk user groups. *In 2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society. Disponível em: https://doi.org/10.1109/SP54263.2024.00027
- Janiszewski, M., et al. (2022). VARIoT—Vulnerability and attack repository for the Internet of Things. *In 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid)*. IEEE. Disponível em: https://doi.org/10.1109/CCGrid54584.2022.00085
- Joinson, A. N., Dixon, M., Coventry, L., & Briggs, P. (2023). Development of a new "human cyber-resilience scale". *Journal of Cybersecurity, 9*(1), Disponível em: https://doi.org/10.1093/cybsec/tyad007
- McCormac, A., Calic, D., Parsons, K., Butavicius, M. A., Pattinson, M. R., & Lillie, M. (2018). The effect of resilience and job stress on information security awareness. I*nformation & Computer Security,* 26(3). Disponível em: https://doi.org/10.1108/ICS-03-2018-0032
- Meissner, F., Wilke, A. J., & Puikytė, M. (2025). How is cybersecurity discussed across media channels? Exploratory analyses of Twitter content and news reporting. *Journal of Risk Research,* 28(8). Disponível em: https://doi.org/10.1080/13669877.2025.2553079
- Pochat, V. L., et al. (2018). Tranco: A research-oriented top sites ranking hardened against manipulation. arXiv preprint *arXiv:1806.01156*. Disponível em: https://arxiv.org/pdf/1806.01156
- Quinlan, M., Ceross, A., & Simpson, A. (2024). The efficacy potential of cyber security advice as presented in news articles. *Interacting with Computers,* 37(1). Disponível em: https://doi.org/10.1093/iwc/iwae048
- Roberts, H., et al. (2021). Media cloud: Massive open source collection of global news on the open web. *In Proceedings of the International AAAI Conference on Web and Social Media,* 15(1). Disponível em: https://doi.org/10.1609/icwsm.v15i1.18127
- Roozenbeek, J., & Van der Linden, S. (2019). Fake news game confers psychological resistance against online misinformation. *Palgrave Communications,* 5(1). Disponível em: https://doi.org/10.1057/s41599-019-0279-9

- Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security, 97.* Disponível em: https://doi.org/10.1016/j.cose.2020.101996
- Smeets, M. (2025). *Ransom war: How cyber crime became a threat to national security.* Oxford University Press & Hurst Publishers.
- van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity, 6*(1). Disponível em: https://doi.org/10.1093/cybsec/tyaa019

LEGISLAÇÃO

[consultadas a 13/02/2026]

- Carta Portuguesa de Direitos Humanos na Era Digital – Lei n.º 27/2021. Diário da República, Série I (17-05-2021), pp. 5 – 10 (alterado). Disponível em: https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2021-164870244
- Lei do cibercrime - Lei n.º 109/2009. Diário da República, Série I, n.º 179 (15-09-2009), pp. 6319 – 6325 (alterado). Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/109-2009-489693
- Regime jurídico da segurança do ciberespaço - Lei n.º 46/2018. Diário da República, Série I (13-08-2018), pp. 4031 – 403. Disponível em: https://dre.pt/dre/detalhe/lei/46-2018-116029384
- Regime jurídico da cibersegurança - Decreto-Lei n.º 125/2025. Diário da República, Série I (04-12-2025). Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/125-2025-962603401
- Regime jurídico dos grau e diplomas do ensino superior - Decreto-Lei n.º 74/2006. Diário da República, Série I-A (24-03-2006), pp. 2242-2257 (alterado). Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/74-2006-671387
- Regulamenta o regime jurídico da segurança do ciberespaço - Decreto-Lei n.º 65/2021. Diário da República, Série I (30-07-2021), pp. 8-21. Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988

WEBSITES

[consultados a 13/02/2026]

- a3es.pt/pt/avaliacao-e-acreditacao/resultados-dos-processo-de-avaliacao-e-acreditacao/acreditacao-de-ciclos-de-estudos/
- https://selosmaturidadedigital.incm.pt/Cybersecurity
- internet.nl
- manrs.org/
- ncsi.ega.ee/
- observatory.isoc.pt/domains.html
- shadowserver.org/
- support.google.com/trends/answer/4365533?hl=en
- trends.google.com/trends/?geo=PT
- www.cisa.gov/known-exploited-vulnerabilities-catalog
- www.cncs.gov.pt
- www.dgeec.medu.pt/p/ensino-superior
- www.dges.gov.pt/pt/pesquisa_cursos_instituicoes
- www.ietf.org
- www.ipac.pt/pesquisa/bdec2.html
- www.mediacloud.org/
- www.nau.edu.pt/pt/

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Observatório
de **Cibersegurança**

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