CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

RELATÓRIO EM 15 MINUTOS

DEZEMBRO 2023

CIBERSEGURANÇA EM PORTUGAL

SOCIEDADE 2023

5ª EDIÇÃO

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

A. SUMÁRIO EXECUTIVO

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

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

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

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

ANÁLISE GLOBAL[1]

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

TENDÊNCIAS

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

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

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

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

ATITUDES E COMPORTAMENTOS

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

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

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

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

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

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

SENSIBILIZAÇÃO E EDUCAÇÃO

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

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

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

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

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

CENÁRIOS DE AMEAÇAS E O FATOR HUMANO

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

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

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

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

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

Quadro 1

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

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

 Contributo negativo para a mitigação da ameaça
 Contributo positivo para a mitigação da ameaça
 Contributo não decisivo para a mitigação da ameaça

ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO 2019-2023

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

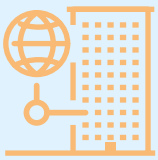
1. Verificam-se tendências positivas nas práticas de sensibilização em cibersegurança, tais como a elevada variedade de canais usados, a especificidade de públicos, bem como uma aplicação mais consistente nas organizações. Persiste uma tendência negativa na falta de avaliação de impacto em muitas das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

DESTAQUES

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

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

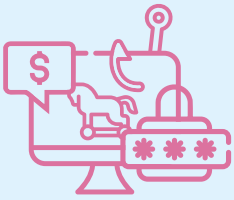
Quase todas as organizações privadas e públicas em Portugal possuem ligações de banda larga à Internet em 2022 (e.g. 100% das Câmaras Municipais) (Eurostat e DGEEC).



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

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

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



ATITUDES E COMPORTAMENTOS EM PORTUGAL

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

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

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

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

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

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

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

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

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

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

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

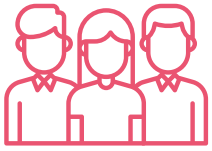
Em 2022, apenas 3% dos organismos do conjunto da Administração Pública tinha seguro contra incidentes de segurança nas TIC (DGEEC).

EDUCAÇÃO E SENSIBILIZAÇÃO EM PORTUGAL

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

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

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



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

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

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

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

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

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

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

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

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

Observatório
de **Cibersegurança**

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

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