CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Observatório de Cibersegurança

RELATÓRIO EM 15 MINUTOS

DEZEMBRO 2022

CIBERSEGURANÇA EM PORTUGAL

SOCIEDADE 2022

4ª EDIÇÃO

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

A. SUMÁRIO EXECUTIVO

A dimensão comportamental da cibersegurança tem mantido a sua relevância, apesar do desenvolvimento tecnológico e das novas soluções digitais de segurança. Os dados mostram que a utilização da vulnerabilidade humana como vetor de ataque no ciberespaço continua a ser muito frequente, conduzindo, por vezes, a grandes impactos (CNCS, 2022a). Por isso, o *Relatório Cibersegurança em Portugal, tema Sociedade*, enquanto o documento do Observatório de Cibersegurança dedicado às atitudes, comportamentos, sensibilização e educação em cibersegurança, continua a merecer uma periodicidade anual na sua publicação, de modo a acompanhar e medir as transformações nesta matéria. A análise, tal como em anos anteriores, sistematiza a informação disponível sobre este assunto e produz aquela que se identifica como estando em falta, apresentando uma visão integrada.

Este relatório divide-se em quatro áreas temáticas relativas a Portugal, com particular incidência em 2021 (mas também com alguns dados de 2022):

1. Ambiente sociotécnico, em que se analisa a evolução dos usos da Internet e serviços digitais;
2. Pesquisas *online*, onde se apresentam dados sobre o interesse pela pesquisa da palavra "cibersegurança";
3. Atitudes e comportamentos, momento em que se expõem os indicadores disponíveis sobre as perceções e as boas práticas relativos à cibersegurança em indivíduos e organizações;
4. Sensibilização e educação, etapa dedicada à evolução das ações de sensibilização em ciber-higiene e aos cursos especializados em cibersegurança e segurança de informação.

Procura-se ainda verificar, ao longo do documento e num capítulo específico, se os indicadores analisados permitem correlações com as linhas de ação da Estratégia Nacional de Segurança do Ciberespaço 2019- 2023 (ENSC), no sentido de ponderar eventuais impactos desta na sociedade portuguesa e necessidades de reajustes na sua execução ou orientações para uma nova estratégia.

ANÁLISE GLOBAL

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

TENDÊNCIAS

AMBIENTE SOCIOTÉCNICO E PESQUISAS *ONLINE*

Verifica-se, em 2021, uma tendência, que já se fazia sentir em 2020, de aumento dos usos da Internet e de alguns serviços críticos para a cibersegurança, como o *email*, o telefone e videochamadas *online*, as mensagens instantâneas, o banco *online* e as compras *online*.

> UMA MAIOR UTILIZAÇÃO DESTAS PLATAFORMAS SIGNIFICA UMA MAIOR EXPOSIÇÃO AOS RISCOS

Ameaças muito frequentes como o *phishing, o vishing, o smishing*, o comprometimento de contas e a burla *online* utilizam estes serviços como superfícies de ataque. Uma maior utilização destas plataformas significa uma maior exposição aos riscos, logo, uma maior necessidade de cuidados.

O termo "cibersegurança" passou a ser mais pesquisado *online* em Portugal a partir de 2020, comparando com 2019, verificando-se uma ligeira descida em 2021 e um aumento significativo no primeiro semestre de 2022. Acontecimentos como a pandemia e ataques muito relevantes a organizações portuguesas podem ter contribuído para este crescimento.

ATITUDES E COMPORTAMENTOS

Verifica-se uma tendência positiva no que se refere ao conhecimento e práticas relativos à gestão dos dados pessoais *online* por parte dos indivíduos. Existe ainda uma discrepância entre perceção e realidade relativamente às compras *online*: a ideia de que a segurança e a privacidade são problemas é muito maior entre os indivíduos que percecionam aí uma barreira às compras *online*, ao ponto de não as realizarem, comparando com os problemas de fraude efetivamente identificados entre os que fazem esse tipo de compras.

As pequenas e médias empresas (PME) portuguesas reconhecem mais que sofrem cibercrimes e revelam mais preocupações quanto aos riscos de os virem a sofrer do que a média da União Europeia (UE), mas também reportam mais os incidentes às autoridades do que a média da UE.

No âmbito da Administração Pública, são notórias algumas tendências negativas: existem menos estratégias para a segurança de informação definidas e uma maior necessidade de reforço das competências em segurança das Tecnologias de Informação e Comunicação (TIC). Mais positivos são os dados que mostram aumentos na aplicação de medidas de segurança das TIC e na disponibilização de recomendações de boas práticas nestes organismos.

SENSIBILIZAÇÃO E EDUCAÇÃO

Existe uma grande predominância, em termos de tipologia de ações de sensibilização em cibersegurança, realizadas por organizações com a missão de efetuar essas ações junto de públicos externos, das sessões presenciais ou *online* comparativamente a outros tipos de ações. Todavia, os cursos *online* mostram uma maior eficácia em termos do número de pessoas alcançadas, o que não significa que tenham melhores efeitos no comportamento. A maioria destas organizações não avalia o impacto das suas ações de sensibilização no comportamento do público-alvo, o qual é sobretudo adulto e sem predomínio de sexo. Os temas mais comuns são os relacionados com boas práticas genéricas de ciber-higiene.

Poucas PME portuguesas realizam ações de sensibilização aos seus funcionários no âmbito da cibersegurança. A Administração Pública efetua essas ações com maior frequência, mas sobretudo de forma voluntária, poucas são obrigatórias. Não obstante, a percentagem deste tipo de ações na Administração Pública está a aumentar.

Verifica-se um crescimento no número de cursos superiores de cibersegurança e segurança de informação, nomeadamente cursos de Técnico Superior Profissional (TESP), e também de alunos inscritos. Há, por outro lado, um decréscimo no número de alunos diplomados. A proporção de mulheres inscritas e diplomadas continua a ser reduzida e apresenta um valor abaixo da proporção de mulheres diplomadas em cursos de TIC em Portugal.

CENÁRIOS DE AMEAÇAS E O FATOR HUMANO

Os anos de 2020 e 2021 foram particularmente marcados pela pandemia da Covid-19 e pelas consequências sociais e económicas da mesma. Como foi verificado em termos de ameaças nos relatórios do Observatório de Cibersegurança dedicados aos *Riscos e Conflitos* 2021 e 2022 (CNCS, 2021a e 2022a), neste período verificou-se um aumento no número de incidentes e cibercrimes. Contudo, a mitigação progressiva da pandemia e o surgimento de uma guerra na Ucrânia fizeram emergir novos fatores de ameaça.

O contexto de pandemia favoreceu as burlas *online*, o comprometimento de sistemas próprios do trabalho remoto (RDP, VPN) e o *phishing*, verificando-se como temáticas dominantes de *phishing* as ligadas à banca, aos transportes e logística e à captura de credenciais de *email*. Por outro lado, com o emergir da guerra na Ucrânia, já em 2022, surgem com um reforço na sua relevância a ciberespionagem, o comprometimento de cadeias de fornecimento, o DDoS e o *phishing* dirigido a pessoas específicas (*spear phishing*), entre outros, com tendência para afetar a Administração Pública e os operadores de serviços essenciais. Em ambos os cenários, algumas ameaças são constantes, como o *ransomware*, por exemplo. Em 2021, em particular, persistiram como ameaças importantes o *phishing/smishing/vishing*, o *ransomware*, a fraude/burla *online*, o comprometimento de contas e a exploração de vulnerabilidades (CNCS, 2022a). Em qualquer dos casos, as fragilidades do fator humano são recorrentemente exploradas como vetores de ataque.

As atitudes, os comportamentos, a sensibilização e a educação são tópicos fundamentais para promover o reforço do fator humano. Considerando as principais conclusões deste relatório e as ameaças mais relevantes de 2021 (ver quadro 1), verifica-se a existência de algumas circunstâncias que têm um contributo negativo para a mitigação das ameaças: o aumento dos usos da Internet e serviços digitais; a diminuição do número de estratégias de segurança de informação e a falta de profissionais da área na Administração Pública; a existência de poucas ações de sensibilização nas PME e, as que se realizam na Administração Pública, serem sobretudo voluntárias; a diminuição do número de diplomados em cursos especializados; e os desequilíbrios sociodemográficos relativamente aos conhecimentos, práticas e ações de sensibilização em cibersegurança. Com um contributo em geral positivo, encontram-se as seguintes situações: a razoável gestão dos dados pessoais *online* por parte dos indivíduos e a sua preocupação com as compras *online* (embora uma preocupação que conduza ao não uso nem sempre seja positiva); a elevada preocupação das PME com os riscos de cibercrime e a significativa tendência para reportarem incidentes; os aumentos na aplicação de medidas de segurança das TIC e na distribuição de recomendações deste âmbito na Administração Pública; o alcance generalizado das ações de sensibilização em cibersegurança em termos temáticos e de público-alvo; e o crescimento do número de cursos e alunos especializados em cibersegurança e segurança de informação.

Algumas ameaças afetam alvos e exigem competências e práticas mais individuais, como a fraude/burla *online*; outras, mais organizacionais, como o *ransomware*; outras ainda, têm um caráter mais técnico, como a exploração de vulnerabilidades; enquanto o *phishing*, por exemplo, depende muito do fator humano. Estas diferenças interferem na relevância de cada boa prática em relação a cada ameaça.

Quadro 1

RELAÇÃO ENTRE RESULTADOS DESTE RELATÓRIO E PRINCIPAIS AMEAÇAS AO CIBERESPAÇO DE INTERESSE NACIONAL, EM 2021

Resultados *Sociedade 2022* / Ameaças *Riscos e Conflitos* 2022 (CNCS, 2022)	Phishing Smishing Vishing	Ransomware	Fraude Burla *online*	Comprometimento de contas	Exploração de vulnerabilidades
Maior risco fruto de aumento dos usos da Internet e serviços digitais					
Melhor gestão dos dados pessoais e elevada preocupação com compras *online*					
Elevada preocupação das PME com riscos e elevado reporte de incidentes					
Menos estratégias de segurança de informação na Administração Pública					
Elevada necessidade de competências de segurança das TIC na Administração Pública					
Mais medidas aplicadas e recomendações distribuídas na Administração Pública					
Alcance genérico das ações de sensibilização em termos temáticos e de público-alvo					
Poucas ações de sensibilização nas PME e poucas obrigatórias na Administração Pública					
Mais cursos especializados e mais alunos a frequentar os mesmos					
Menos diplomados em cursos especializados					
Desequilíbrios sociodemográficos nos conhecimentos, práticas e sensibilização					

 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

No âmbito do acompanhamento da ENSC, é possível identificar cinco grandes domínios com os quais os resultados deste Relatório se relacionam e em que é possível identificar aspetos positivos e negativos, em particular no que diz respeito ao Eixo 2 - Prevenção, educação e sensibilização e, em parte, ao Eixo 1 - Estrutura de segurança do ciberespaço.

1. Relativamente à sensibilização do cidadão em geral, embora existam dados positivos quanto a alguns comportamentos, as ações de sensibilização nas organizações são insuficientes ou apenas voluntárias. As ações de sensibilização que se dirigem ao cidadão em geral têm um peso elevado de temas genéricos de cibersegurança e tendem a não se restringir a um público-alvo específico, aspeto positivo no que se refere ao alcance.
2. No que diz respeito à sensibilização de grupos específicos, persistem desequilíbrios sociodemográficos, em que os adultos mais velhos e as pessoas com menos formação têm menos conhecimentos e cuidados de ciber-higiene. As ações de sensibilização tendem a não focar suficientemente grupos específicos, nomeadamente adultos mais velhos.
3. Quanto ao objetivo de introduzir o tema da cibersegurança na educação formal, o aumento de cursos especializados e de alunos é um dado positivo, embora haja menos diplomados.
4. Quanto à necessidade de qualificação de especialistas, verifica-se que esta necessidade persiste elevada na Administração Pública em particular.
5. Por fim, considerando as linhas de ação que promovem a colaboração entre entidades na reação a incidentes, a tendência das PME portuguesas para reportarem incidentes é positiva.

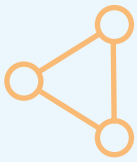
DESTAQUES

AMBIENTE SOCIOTÉCNICO E PESQUISAS *ONLINE* SOBRE "CIBERSEGURANÇA" EM PORTUGAL

Verificou-se um aumento do uso da Internet em 4 pp, de 78% dos indivíduos em 2020 para 82% em 2021. Ainda assim, este valor é menor em 7 pp do que a média da UE (Eurostat).

Há mais indivíduos a usar alguns serviços *online* críticos em 2021 do que em 2020: o *email* (88% - mais 1 pp e 3 pp acima da média da UE); o telefone e videochamadas *online* (80% - mais 10 pp e 7 pp acima da média da UE); as mensagens instantâneas (91% - mais 1 pp e 12 pp acima da média da UE); banco *online* (64% - mais 4 pp e 2 pp abaixo da média da UE); e as compras *online* (40% - mais 5 pp e 17 pp abaixo da média da UE) (Eurostat).

As redes sociais, embora não sejam mais usadas em 2021 do que em 2020, mantêm-se a ser usadas por 80% dos indivíduos em Portugal, mais 16 pp do que a média da UE, que é de 64% (Eurostat).



As pesquisas *online* pela palavra "cibersegurança" aumentaram de forma significativa em 2020, diminuindo ligeiramente em 2021. Em 2022, voltaram a aumentar no primeiro semestre de forma muito significativa (Google Trends).

Os distritos de Lisboa, Setúbal e Coimbra são as regiões com mais interesse pela pesquisa da palavra "cibersegurança" a nível nacional, proporcionalmente em relação à dimensão de cada uma destas regiões (Google Trends).

Os termos paralelos (não sinónimos de "cibersegurança") mais relevantes nestas pesquisas são "CNCS" e os ligados ao tema da educação, como "disciplina" e "mestrado" (Google Trends).

ATITUDES E COMPORTAMENTOS EM PORTUGAL

Verifica-se uma tendência positiva, em 2021, relativamente ao conhecimento que os indivíduos possuem sobre os *cookies*, com 63% de respostas positivas, uma melhoria de 4 pp comparando com 2020. Ainda assim, 9 pp abaixo da média da UE (Eurostat).

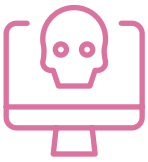
Em 2021, existem mais cuidados com a gestão dos dados pessoais *online* por parte dos indivíduos do que em 2020 (71% utiliza pelo menos um método de gestão - mais 3 pp), valor acima da média da UE (em 6 pp) (Eurostat).

As pessoas mais velhas e as que têm formação básica demonstraram, em 2021, ter menos cuidados com a privacidade e a proteção de dados pessoais *online* do que os jovens e do que as pessoas com formação superior. No entanto, as pessoas com formação básica percecionaram mais barreiras às compras *online* devido a preocupações de segurança do que as que têm formação superior (Eurostat).

Os indivíduos, em 2021, percecionaram como barreiras às compras *online* as preocupações de segurança e privacidade em maior volume do que a média da UE (27% em Portugal e 6% na média da UE). Contudo, apenas 1% dos que compraram *online* encontraram problemas de fraude (em Portugal e na média da UE) (Eurostat).

Há menos inquiridos com funções de topo nas PME portuguesas, em 2021, a sentirem-se bem informados sobre os riscos de cibercrime do que a média da UE (67% - menos 4 pp do que a média da UE) (Eurobarómetro).

As PME portuguesas, em 2021, mostram-se mais preocupadas com os riscos *online* do que a média da UE (e. g., 55% estão preocupadas com o *hacking* a contas bancárias *online*, enquanto a média da UE é de 32%) (Eurobarómetro).



Há mais PME portuguesas, em 2021, a admitirem ter sofrido pelo menos um cibercrime nos últimos 12 meses (48%) do que a média da UE (28%) (Eurobarómetro).

Em 2021, o impacto mais sentido pelas PME portuguesas como resultado do incidente mais grave foi a impossibilidade de uso de recursos ou serviços (para 32%). Na média da UE foi o tempo despendido a responder ao incidente (35%) (Eurobarómetro).

As PME portuguesas, em 2021, reportaram mais incidentes do que a média da UE (81% em Portugal e 54% na média da UE). A entidade a quem mais reportaram foi a polícia (24%) e, quando não reportaram, a razão mais apresentada foi considerarem o caso demasiado trivial (27%) (Eurobarómetro).

A percentagem de organismos da Administração Pública com uma estratégia para a segurança de informação definida diminuiu em 2021, comparando com 2020, em 2 pp, fixando-se em 59% (DGEEC).

Em 2021, há mais organismos da Administração Pública a aplicarem medidas de segurança das TIC, com particular destaque para a Administração Regional da Madeira (DGEEC).

Existem mais organismos da Administração Pública, em 2021, a indicarem ter elevada necessidade de reforço de competências em segurança das TIC, fixando-se em 69%, mais 7 pp do que no ano anterior (DGEEC).

Nas Câmaras Municipais do Norte do país, em 2021, verifica-se alguma correlação entre a existência de uma elevada necessidade de reforço de competências em segurança das TIC e a ausência de estratégias para a segurança de informação definidas. Na Área Metropolitana de Lisboa essa correlação não existe, indiciando-se uma correlação inversa (DGEEC).

Predomina pessoal do próprio organismo, na Administração Pública, na realização de atividades relacionadas com a segurança das TIC, em 2021 (entre 40% e 51%) (DGEEC).

O número de entidades da Administração Pública com recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC aumentou 2 pp em 2021, verificando-se em 47% das mesmas (DGEEC).

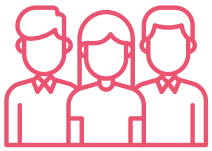
Há menos entidades da Administração Pública com seguro contra incidentes de segurança das TIC, tendo passado de 5% em 2020 para 3% em 2021 (DGEEC).

EDUCAÇÃO E SENSIBILIZAÇÃO EM PORTUGAL

A maioria das ações de sensibilização em cibersegurança realizadas por entidades com responsabilidades na matéria, em 2021, ocorreram através de sessões presenciais ou *online* (80%). Seguem-se as redes sociais (7,4%), os cursos *online* (6,4%) e outros meios como *websites* (6,2%). Há muito poucas ações nos meios de comunicação social (0,1%) (CNCS).

Em 2021, comparando as sessões presenciais ou *online* com os cursos *online* de sensibilização em cibersegurança, estes revelam alguma eficácia em termos do número de pessoas alcançadas (CNCS).

Os jovens adultos (19-29 anos) e os adultos (30-64) foram as faixas etárias que predominaram como públicos-alvo das ações de sensibilização em cibersegurança, em 2021 e 2022 (até ao 1o semestre). Não se verifica o predomínio de um sexo. (CNCS).



Os temas que predominaram como conteúdos das ações de sensibilização em cibersegurança, em 2021 e 2022 (até ao 1o semestre), foram as "Boas práticas genéricas de ciber-higiene", os "Riscos *online* e cibercrime" e a "Proteção de dados, privacidade e direitos" (CNCS).

Somente 33% das organizações estudadas que realizaram ações de sensibilização em cibersegurança, em 2021 e 2022 (até ao 1o semestre), analisaram os impactos das mesmas no comportamento dos seus públicos-alvo (CNCS).

Somente 22% das PME em Portugal realizou ações de formação ou de consciencialização para os seus funcionários sobre os riscos do cibercrime, nos últimos 12 meses, em 2021. Este valor, ainda assim, é superior à média da UE, que se fixa em 19% (Eurobarómetro).

Na Administração Pública, em 2021, as ações de formação dos funcionários para a consciencialização das suas obrigações em matéria de segurança das TIC foram, na sua maioria, voluntárias, estando estas presentes em 67% dos organismos (mais 2 pp do que no ano anterior). As ações obrigatórias aumentaram a sua percentagem de 22% em 2020 para 26% em 2021 (DGEEC).

Registaram-se mais 3 cursos superiores especializados em cibersegurança e segurança de informação em Portugal, em 2022, todos eles TESP, perfazendo um total de 25: 13 TESP, uma licenciatura, 10 mestrados e um doutoramento (DGES: recolha CNCS).

Em termos de distribuição regional, em 2022, 44% dos cursos especializados em cibersegurança e segurança de informação concentram-se no Norte do país, 28% na Área Metropolitana de Lisboa, 20% no Centro e 8% no Alentejo (DGES: recolha CNCS).

Verificou-se um crescimento de 28% no número de alunos inscritos em cursos especializados em cibersegurança e segurança de informação no ano letivo de 2021/2022, de 718 para 916. Entre os alunos inscritos, 10% são mulheres (mais 2 pp do que no ano anterior) (DGEEC: recolha CNCS).

No ano letivo de 2020/2021, o número de alunos diplomados em cursos especializados em cibersegurança e segurança de informação decresceu 14%, de 152 para 130. Entre os alunos diplomados, 6% são mulheres (menos 3 pp do que no ano anterior) (DGEEC: recolha CNCS).

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