COMUNICADO DE IMPRENSA

Relatório Cibersegurança em Portugal, tema Sociedade

Documento identifica o estado da resiliência da sociedade portuguesa face às ciberameaças

Lisboa, 30 de abril, 2026 – Está disponível a 7.ª edição do Relatório Cibersegurança em Portugal, tema Sociedade, um documento desenvolvido pelo Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS), que analisa a componente social da cibersegurança, abrangendo indivíduos, famílias, empresas e organismos da administração pública.

Esta edição do Relatório apresenta uma alteração substancial na metodologia analítica usada, em resultado de um realinhamento do objetivo principal do documento — passa a centrar-se na identificação do estado da resiliência da sociedade portuguesa face às ciberameaças, organizando a análise em três dimensões:

1) o estado da ameaça;
2) a superfície de ataque;
3) a ciber-resiliência.

Esta análise procura responder a uma **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)?

Mantendo as principais fontes de dados utilizadas nas edições anteriores, nesta edição acrescentaram-se novas fontes de dados produzidos por várias entidades públicas e privadas, nacionais e internacionais. O relatório inclui, ainda, dados originais recolhidos e produzidos pelo Observatório de cibersegurança, especificamente para este relatório.

Um dos objetivos desta edição é que que seja lida em complementaridade com o Relatório Cibersegurança em Portugal, tema Riscos & Conflitos (publicado em 2025), que permitindo uma visão integrada do panorama dos riscos no ciberespaço de interesse nacional e da exposição da sociedade portuguesa aos mesmos.

Destacam-se os **principais resultados:**

- O aumento da exposição digital de indivíduos e das famílias eleva o risco de ciberataques, em particular nos domínios da engenharia social e da fraude;

- A digitalização das empresas portuguesas tem sido acompanhada pela adoção de medidas de segurança das TIC (Tecnologias de Informação e Comunicação), mas a maioria não atingiu, ainda, níveis elevados de maturidade;
- Apesar dos progressos significativos na digitalização da administração pública e do elevado grau de adoção de medidas de segurança, estas têm-se revelado insuficientes para evitar incidentes com grande impacto nacional;
- Portugal está longe do grupo de países da União Europeia com mais endereços de IP vulneráveis por habitante, mas também daqueles que registam menos vulnerabilidades.
- Apesar dos avanços recentes, a adoção de normas técnicas e tecnologias de segurança na utilização da Internet e do correio eletrónico, permanece incompleta em Portugal, comprometendo a segurança dos utilizadores;
- O crescente reconhecimento da importância da cibersegurança, embora positivo, ainda não é suficiente para evitar impactos negativos na utilização de produtos e serviços digitais por parte dos cidadãos;
- A perceção de exposição às ciberameaças mantém-se elevada, apesar do reforço de capacidades técnicas e humanas, incluindo o recurso crescente a prestadores externos para colmatar dificuldades de recrutamento;
- As empresas e as universidades ainda não apostam, respetivamente, em ações de sensibilização e formação obrigatórias em cibersegurança.

Das **principais conclusões** dentro dos domínios analisados, destacam-se:

- **Exposição:** elevada exposição digital dos utilizadores e organizações à internet e certos serviços digitais;
- **Nível de interesse em torno do tema:** destaque crescente nos meios de comunicação e índices de pesquisa *online* de ciberameaças relevantes ligadas ao fator humano;
- **Atitudes e comportamentos:** elevada sensibilidade das organizações relativamente à cibersegurança, embora tenham poucos recursos internos;
- **Sensibilização e educação:** pouco uso de meios de grande alcance para campanhas de sensibilização em cibersegurança, mas maior investimento das organizações em ações dirigidas aos colaboradores. Continua a aumentar o número de cursos e alunos de cibersegurança no ensino superior.

Face aos riscos e vulnerabilidades associados às tendências, o relatório identifica **recomendações para as organizações e indivíduos:**

- Associar a literacia digital nas escolas e outros contextos educativos a uma literacia para a cibersegurança;
- Promover boas práticas nas organizações, nomeadamente o uso do da autenticação multifator (MFA), de forma mais acentuada;
- Capacitar mais os recursos das organizações em cibersegurança, nomeadamente na Administração Pública e pequenas e médias empresas (PME);
- Aumentar o alcance das ações de sensibilização chegando a um público mais alargado.

Consulte *a versão integral do estudo*

Para mais informações:

Clara Santos Silva
Comunicação e Imagem do Centro Nacional de Cibersegurança
Tlm: +351 919 592 662 | *comunicacao@cncs.gov.pt*