2025: Um novo capítulo para a cibersegurança em Portugal?

Visão · 2025-02-07



O sucesso desta jornada irá depender de um esforço coletivo entre indivíduos, empresas e governo

---

---

file: 2025-02-07-visao-2025-um-novo-capitulo-para-a-ciberseguranca-em-portugal.md

title: "2025: Um novo capítulo para a cibersegurança em Portugal?"

outlet: Visão

date: 2025-02-07

date_display: "7 de fevereiro de 2025, 18:37 (Europe/Lisbon)"

url: "https://visao.pt/opiniao/2025-02-07-2025-um-novo-capitulo-para-a-ciberseguranca-em-portugal/"

author_page: "https://visao.pt/autores/joao-luis/"

byline: João Luís

affiliation: VP of Engineering da Dashlane

text_status: full

section: Opinião

extract: visao-feb

notes: "A Visão acrescenta no final da página: «Os textos nesta secção refletem a opinião pessoal dos autores. Não representam a VISÃO nem espelham o seu posicionamento editorial.»"

word_count: 956

2025: Um novo capítulo para a cibersegurança em Portugal?

João Luís, VP of Engineering da Dashlane

Visão, 7 de fevereiro de 2025, 18:37 (Europe/Lisbon)

https://visao.pt/opiniao/2025-02-07-2025-um-novo-capitulo-para-a-ciberseguranca-em-portugal/

Nos últimos anos, a área da cibersegurança tem passado por transformações significativas, impulsionadas tanto pela evolução tecnológica como pela

necessidade de resposta a ameaças cada vez mais surpreendentes. A par com avanços importantes, como a crescente adoção de métodos de autenticação mais seguros, o desenvolvimento de ferramentas para ataques de cibersegurança altamente sofisticados tem trazido para cima da mesa desafios bastante complexos.

Com estes avanços e desafios em mente, a cibersegurança em Portugal prepara-se para iniciar um novo capítulo, com a transposição da Diretiva sobre a Segurança das Redes e da Informação 2 (NIS2) para a legislação nacional. Esta mudança, que ampliará significativamente o leque de setores obrigados a adotar medidas rigorosas de segurança, trará, com certeza, uma nova dinâmica ao mercado. De realçar que a NIS2 vai além das exigências da sua antecessora, reconhecendo setores como saúde e finanças como sendo críticos para o funcionamento do país e impondo novas responsabilidades a estas indústrias-chave. A adoção da NIS2 exigirá, assim, um reforço significativo na resiliência empresarial, tornando a cibersegurança numa prioridade estratégica para o país.

À medida que alguns setores são desafiados a adotar práticas de cibersegurança mais robustas, um dos grandes desafios mantém-se: o facto de o tecido empresarial português ser constituído maioritariamente por Pequenas e Médias Empresas (PMEs), que continuam a ser um dos alvos mais vulneráveis a ciberameaças, devido à sua falta de preparação e recursos limitados para as enfrentar. Muitas destas ainda operam com infraestruturas desatualizadas, políticas de segurança insuficientes e falta de sensibilização entre os colaboradores para os riscos digitais. Este último fator é especialmente crítico, considerando que a insider-threat (ameaça interna) se tem tornado num dos maiores riscos para a segurança das empresas. Muitas vezes, os próprios colaboradores – intencionalmente ou não – tornam-se alvos fáceis para os cibercriminosos, que conseguem comprometer dados e sistemas internos ao obter acesso às suas credenciais.

Além disso, a perceção errada de que apenas as grandes organizações são alvo de ciberataques contribui para uma postura reativa – em vez de proativa – à segurança. Nos próximos meses, acredito que as PMEs se tornem cada vez mais

sensíveis e abertas à adoção de práticas de segurança acessíveis e eficazes. O apoio do governo será crucial para elevar o nível de maturidade em cibersegurança desta parte do tecido empresarial, tão essencial para a economia portuguesa.

O rápido avanço da IA tem também vindo a ampliar o panorama das ciberameaças, criando um cenário ainda mais complexo para empresas com recursos limitados e trazendo novos desafios para a segurança da identidade online. Ferramentas de IA generativa, como o ChatGPT, estão a ser exploradas por cibercriminosos para desenvolver ataques de phishing altamente sofisticados. Estes ataques utilizam modelos de linguagem avançados para gerar de forma automatizada mensagens convincentes e personalizadas, tornando-se mais difíceis de identificar e aumentando a sua eficácia.

E, se os ataques alimentados por IA já representam uma ameaça significativa no geral, a evolução das técnicas de social engineering vai ainda mais além, graças ao avanço de tecnologias como deepfake e vishing (voice phishing). A capacidade de criar vídeos e áudios altamente realistas permite que os cibercriminosos imitem com precisão vozes e rostos – como de colegas de trabalho, amigos e até familiares -, tornando as tentativas ainda mais convincentes e bem sucedidas. Esta evolução representa um enorme desafio para empresas e indivíduos, uma vez que os métodos tradicionais de verificação de identidade podem já não ser suficientes para distinguir entre interações legítimas e fraudulentas.

Esta crescente sofisticação das ameaças digitais e a rápida evolução das ferramentas de IA tem posto a nu a escassez de talento qualificado na área, que continua a ser um dos principais desafios para o setor tecnológico nacional e exige uma resposta estratégica por parte das empresas e do governo. Prevejo, nos próximos tempos, uma aposta na requalificação de profissionais para lidar com os novos fatores de risco. Iniciativas como parcerias entre o setor público e privado e incentivos à especialização podem contribuir para reduzir este gap de competências. É provável que as empresas adotem, também elas, ferramentas sofisticadas baseadas em IA, mas para sua própria defesa, permitindo a deteção proativa de ameaças e uma reação rápida a ciberataques.

Perante todo este cenário, a procura por soluções de segurança mais eficazes e acessíveis tem levado à adoção de novas metodologias que simplifiquem a experiência do utilizador. As passkeys são exemplo disso mesmo, sendo que a minha expectativa é que estas continuem o seu caminho em direção à adoção em massa, tanto no contexto pessoal como empresarial. A experiência de login – que não é apenas mais simples, como também mais segura – promete tornar este no método preferido de autenticação, reduzindo significativamente o risco de ciberataques e de credenciais perdidas/roubadas. Com os sistemas operativos e os browsers a oferecer já suporte nativo para passkeys, 2025 poderá ser mesmo o ano de viragem.

Acredito que o futuro da cibersegurança em Portugal será marcado por uma adaptação contínua às novas exigências tecnológicas e regulatórias. Espero que as empresas, especialmente as PMEs, fortaleçam as suas muralhas através da implementação de práticas de segurança mais eficazes. Espero também que os recentes incidentes – como o comprometimento de milhares de credenciais de acesso ao Portal das Finanças – impulsionem mudanças significativas no setor público. A esperança é que o governo português tenha a capacidade de se modernizar e de se tornar num exemplo no que diz respeito à adoção de mecanismos de autenticação mais seguros, até porque este terá um papel crucial na transição para este novo capítulo e na criação de um ambiente que fomente simultaneamente a inovação e a segurança. O sucesso desta jornada irá depender de um esforço coletivo entre indivíduos, empresas e governo, rumo a um ecossistema tecnológico nacional mais seguro e competitivo.

Recovery notes

A Visão acrescenta no final da página: «Os textos nesta secção refletem a opinião pessoal dos autores. Não representam a VISÃO nem espelham o seu posicionamento editorial.»