A IA e o futuro da cibersegurança empresarial

Jornal Económico · 2025-12-02



No fundo, a cibersegurança não se constrói apenas com tecnologia; é um desafio de liderança, cultura e compromisso coletivo.

---

file: 2025-12-02-jornal-economico-a-ia-e-o-futuro-da-ciberseguranca-empresarial.md

title: A IA e o futuro da cibersegurança empresarial

outlet: Jornal Económico

date: 2025-12-02

date_display: "2 de dezembro de 2025, 00:08 (Europe/Lisbon)"

url: "https://jornaleconomico.sapo.pt/noticias/a-ia-e-o-futuro-da-ciberseguranca-empresarial/"

author_page: "https://jornaleconomico.sapo.pt/noticias/author/joao-luis-vp-of-engineering-da-dashlane/"

byline: João Luís, VP of Engineering da Dashlane

affiliation: VP of Engineering da Dashlane

text_status: full

section: Opinião

extract: je

word_count: 938

A IA e o futuro da cibersegurança empresarial

João Luís, VP of Engineering da Dashlane

Jornal Económico, 2 de dezembro de 2025, 00:08 (Europe/Lisbon)

https://jornaleconomico.sapo.pt/noticias/a-ia-e-o-futuro-da-ciberseguranca-empresarial/

Em 2024, o impacto financeiro de uma violação de dados atingiu um valor recorde, com um custo médio global de 4,88 milhões de dólares. Até 2028, estima-se que o cibercrime venha a custar cerca de 13,8 biliões de dólares às empresas. Na Europa, prevê-se que o impacto direto das ciberameaças tenha um crescimento de 64% até 2029.

Neste cenário de agravamento dos prejuízos causados pelo cibercrime, a Inteligência Artificial (IA) surge como a principal ameaça e desafio, ao permitir ataques mais elaborados e difíceis de detetar, nomeadamente de engenharia social, como deepfakes incrivelmente realistas. Além disso, a IA facilita a geração em grande escala de ataques de phishing e conta com uma rápida capacidade de adaptação, tornando a reação e a mitigação num enorme desafio para as empresas. Entre 2023 e 2024, a utilização de IA generativa em ciberataques disparou 600%, um sinal claro da crescente sofisticação e escala destas ameaças.

Estes números revelam apenas uma parte da gravidade e complexidade do problema, mas já são suficientes para revelar um cenário alarmante que obriga a olhar de perto para os fatores que o explicam. Entre estes, estão o facto de os ataques de ransomware serem cada vez mais avançados e difíceis de contornar, assim como a crescente digitalização das operações empresariais.

A adoção da computação em nuvem (cloud), o aumento do trabalho remoto e a proliferação de dispositivos IoT (Internet of Things) ampliam a superfície de ataque. Paralelamente, o setor continua a deparar-se com a falta de profissionais especializados, juntando-se o aumento dos salários e dos custos operacionais. A IA completa naturalmente este quadro, ao proporcionar métodos inovadores para a concretização de ataques.

Em Portugal, a maturidade das empresas na preparação e resposta a incidentes de cibersegurança ainda está longe de ser ideal, sobretudo entre as pequenas e médias empresas (PMEs), que representam 99,9% do tecido empresarial. Estas estão mesmo entre os principais alvos de ciberataques (ao contrário do que as próprias, muitas vezes, acham) e, frequentemente, não têm proteção adequada, enfrentando obstáculos significativos como recursos financeiros limitados e falta de conhecimento especializado.

Muitas vezes, a cibersegurança é relegada para segundo plano em favor do foco no core business. As poucas exceções a esta regra são algumas grandes empresas, especialmente as reguladas ou do setor público, que têm obrigatoriamente estruturas dedicadas como CISOs (Chief Information Security

Officers) e responsáveis de risco.

Para a maioria, o caminho ainda passa pelo reforço das medidas mais básicas: formação interna, backups regulares, implementação de firewalls, utilização de gestores de passwords, atualização constante de software e definição de planos de resposta concretos e testados para incidentes.

A resposta da UE às novas ameaças

O novo quadro legal europeu, em particular a diretiva NIS2, promete um alinhamento mais rigoroso das empresas com as boas práticas de cibersegurança. Em Portugal, o Governo já aprovou, em Conselho de Ministros, o decreto-lei que transpõe esta diretiva, concluindo o processo legislativo que estava pendente desde o início do ano. O diploma estabelece a obrigatoriedade de medidas de prevenção, resposta e recuperação para empresas de todas as dimensões e setores, bem como padrões mais elevados para a segurança dos sistemas e dados empresariais.

Neste domínio das políticas públicas e da cooperação internacional, iniciativas como a diretiva NIS2 e o Cyber Resilience Act (CRA) vão estabelecer um novo patamar de exigência no campo da cibersegurança. Ao colocar a responsabilidade diretamente nos conselhos de administração e impor frameworks mais robustas em todos os setores, espera-se, finalmente, criar um ambiente onde a cibersegurança passará a ser imprescindível e inegociável. Esta exigência torna-se ainda mais crítica face ao avanço da IA, que eleva o nível das ameaças e obriga à implementação de estratégias de defesa ágeis e sólidas.

A verdade é que o real custo de um ciberataque vai muito além de questões como o resgate monetário pago em ataques de ransomware. Casos como o ataque à AMA (Agência para a Modernização Administrativa), em que a recuperação dos sistemas demorou mais de um mês, mostram a verdadeira extensão dos custos envolvidos: resposta técnica, recursos humanos, software, multas regulatórias, custos legais e prejuízos na produtividade.

A tudo isto soma-se ainda o impacto na credibilidade das organizações, consequência direta da exposição de dados sensíveis dos cidadãos por parte de instituições cuja missão é precisamente protegê-los. O tempo de inatividade é mesmo um dos fatores mais dispendiosos, com impacto direto nas receitas. Outros fatores, como danos reputacionais e perda de confiança dos clientes, podem também ser devastadores para o futuro do negócio.

Para além das soluções técnicas, a cultura organizacional também tem um papel decisivo na cibersegurança. A principal ameaça para as empresas continua a ser a insider threat: a grande maioria dos ataques começa com a exploração inadvertida de um colaborador que, muitas vezes sem conhecimento, facilita o acesso dos hackers aos sistemas empresariais. É por isso que a responsabilidade não deve pertencer exclusivamente aos departamentos de TI, mas ser transversal a toda a organização, a começar pelo topo. A responsabilização legal direta dos diretores executivos, introduzida pela NIS2, é um elemento que facilita esse compromisso, tornando a cibersegurança numa prioridade estratégica definitiva.

No fundo, a cibersegurança não se constrói apenas com tecnologia; é um desafio de liderança, cultura e compromisso coletivo. O futuro será das organizações que entenderem esta exigência e se tornarem verdadeiramente ciber-resilientes. Agora que o decreto-lei que transpõe a NIS2 foi aprovado no nosso país, o foco deve estar na implementação prática e na fiscalização efetiva das novas regras, garantindo que as empresas dispõem de meios, prazos e orientação adequada para cumprir o novo regime. Este será um passo decisivo para garantir que as novas exigências se transformem em ações efetivas.