Será 2026, finalmente, o ano da cibersegurança?

Visão · 2025-12-27



Já não basta reforçar a firewall ou promover uma ação pontual de formação

---

file: 2025-12-27-visao-sera-2026-finalmente-o-ano-da-ciberseguranca.md

title: Será 2026, finalmente, o ano da cibersegurança?

outlet: Visão

date: 2025-12-27

date_display: "27 de dezembro de 2025, 10:08 (Europe/Lisbon)"

url: "https://visao.pt/opiniao/ponto-de-vista/2025-12-27-sera-2026-finalmente-o-ano-da-ciberseguranca/"

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

byline: João Luís

affiliation: VP of Engineering da Dashlane

text_status: full

section: Opinião / Ponto de vista

extract: visao-dec

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: 970

Será 2026, finalmente, o ano da cibersegurança?

João Luís, VP of Engineering da Dashlane

Visão, 27 de dezembro de 2025, 10:08 (Europe/Lisbon)

https://visao.pt/opiniao/ponto-de-vista/2025-12-27-sera-2026-finalmente-o-ano-da-ciberseguranca/

Será que o próximo ano é, de uma vez por todas, o ano em que deixamos de falar de cibersegurança apenas quando acontece um incidente e passamos a encará-la como parte natural das decisões de negócio? A pergunta pode parecer repetitiva, mas o contexto joga a favor dessa mudança estrutural: a transposição da NIS2

para a lei portuguesa, a crescente exposição mediática dos ciberataques e a maturidade tecnológica das próprias empresas empurram o tema para um novo patamar.

Quando olho para o próximo ano, diria que a mudança não será necessariamente tecnológica, mas mental. Já não basta reforçar a firewall ou promover uma ação pontual de formação; quem quiser ser competitivo em 2026 terá de provar, na prática, que consegue proteger dados, operações e identidade digital com o mesmo rigor com que gere outras áreas do negócio.

Será 2026 o ano em que a cibersegurança passa de custo a alavanca estratégica?

Tudo aponta para que sim. A cibersegurança estará cada vez menos restringida às equipas de TI e cada vez mais no centro das decisões empresariais. A NIS2 vai obrigar mais setores a demonstrarem níveis mínimos de maturidade na área e trazer o tema para a agenda estratégica, transformando-o numa condição para participar em determinados ecossistemas de negócio, especialmente em áreas críticas.

Na prática, decisões como escolher fornecedores passarão a ter a cibersegurança como critério fundamental. Grandes empresas e operadores de serviços irão passar a impor requisitos de segurança (auditando práticas, pedindo evidências de formação e exigindo planos de resposta minimamente estruturados) aos seus fornecedores e parceiros, em particular às PMEs, ainda o elo mais fraco do tecido empresarial português.

Essa pressão top-down pode ser um dos motores mais fortes da profissionalização do setor, obrigando muitas empresas a investir em tecnologia, processos e talento na área – não apenas para evitar multas e incidentes, mas para continuarem competitivas e relevantes no mercado. Em paralelo, é expectável que comecemos a ver um número crescente de startups focadas em formação e capacitação em cibersegurança.

Será 2026 o ano em que a cibersegurança se afirma como pilar da cultura e da operação empresarial?

Também aqui tudo indica que sim, ainda que de forma gradual. A transformação passará pela forma como as equipas operam diariamente, com mais automação e IA na deteção e resposta a incidentes, e com a limitação do impacto do ataque antes de este se tornar num problema sistémico. A segmentação de redes internas, para reduzir a superfície de ataque, e a revisão das políticas de acesso – mitigando insider threats – vão ganhar protagonismo.

A escala dos ataques vai continuar a aumentar, graças a IA generativa, deepfakes e campanhas de phishing altamente personalizadas, obrigando as empresas a responder ao mesmo nível: com sistemas capazes de isolar automaticamente utilizadores e endpoints comprometidos, limitar movimentos laterais e dar tempo às equipas para avaliarem o impacto real de cada incidente. Ao mesmo tempo, ganha peso uma dimensão ainda subvalorizada: ataques em ambiente digital com impacto direto em infraestruturas físicas, como redes de energia, sistemas industriais ou transportes, onde um ciberataque pode paralisar operações ou interromper serviços essenciais.

As grandes organizações vão liderar a resposta: muitas já estão a testar soluções, a investir em exercícios de simulação, planos de continuidade de negócio e mecanismos de recuperação de dados. Começam também a treinar de forma mais consistente a sua força de trabalho, tornando a formação contínua e a cultura de segurança como parte integrante da operação diária.

Será 2026 o ano em que repensamos a dependência de gigantes tecnológicos?

Acho que será, sim, o início de uma nova abordagem. A dependência quase cega de grandes fornecedores de cloud e infraestruturas digitais começará a ser revista com mais pragmatismo. Os apagões recentes de serviços globais associados a grandes empresas tecnológicas – como Cloudflare, Microsoft e Amazon – mostraram o que acontece quando há dependência de um número muito reduzido de fornecedores.

A resposta mais provável passará por arquiteturas híbridas, diversificação de fornecedores e estratégias multi-cloud, bem como planos de continuidade de negócio pensados para isolar e recuperar sistemas críticos em caso de falha

generalizada, assumindo, desde logo, a necessidade de recuperar dados e operações a partir de fontes alternativas. Esta discussão já está até a surgir no setor público, com a criação de estruturas de crise para responder a novos incidentes de grande escala.

Será 2026 o ano em que começamos, de facto, a despedir-nos das passwords?

Talvez ainda não seja o funeral, mas será provavelmente o velório. A adoção de passkeys tem vindo a crescer, suportada nativamente pelos principais sistemas operativos e browsers, e tudo indica que esta tendência se vai consolidar tanto no contexto pessoal como profissional. A possibilidade de oferecer uma experiência de login mais simples, resistente a phishing e independente da memória e da vulnerabilidade do utilizador é demasiado apelativa para ser ignorada, sobretudo num cenário em que o custo dos incidentes de credenciais comprometidas continua a aumentar.

É possível que 2026 fique marcado como o ano em que muitas empresas dão o primeiro passo sério rumo a um futuro passwordless, pelo menos em aplicações críticas. Em simultâneo, a discussão em torno da identidade digital segura vai acelerar, com as passkeys a assumirem um papel central na transição para modelos de autenticação mais robustos e menos dependentes dos hábitos dos utilizadores.

Se, durante anos, só falávamos de cibersegurança quando algo corria mal, 2026 será o ano em que essa tendência fica para trás. A partir do momento em que a segurança passa a pesar nas decisões de negócio, cada organização terá de decidir se fica do lado dos que apenas reagem aos incidentes ou dos que abordam a cibersegurança com uma mentalidade preventiva e como argumento de confiança e de crescimento. No próximo ano, continuar a tratar a segurança apenas como um custo inevitável será, esse sim, o maior risco de todos.

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.»