

bilingual edition

ptsoc{news}

Segundo semestre 2026 | Second half of 2026

#20

Cibersegurança na era da IA

Cybersecurity in the AI Age

Soberania tecnológica: a nova urgência europeia
Technological Sovereignty: The new European urgency

Entre a defesa da soberania e o risco de isolamento
Between defending sovereignty and the risk of isolation

Quando um domínio expira
When a domain expires

Formação em Cibersegurança
Cybersecurity training

Ficha técnica

Credits

Esta publicação é produzida pelo .pt
This publication is produced by .pt

20ª Edição | Segundo semestre 2026
20th Edition | Second half of 2026

Edição e design gráfico: Casa dos Bits – Edições Lda.
Edited and designed by: Casa dos Bits – Edições Lda



Conteúdos deste documento ao abrigo da Licença Creative Commons - Atribuição-Não Comercial 4.0 Internacional. Ele pode ser copiado e redistribuído por qualquer meio ou formato, misturado, transformado e usado para a elaboração de outro material que deverá ser distribuído usando a mesma licença. Para mais detalhes consultar as condições de uso em <http://creativecommons.org/licenses/by/4.0/>
Todos os direitos reservados PTSOC News.

Índice

Cibersegurança na era da IA: entre a velocidade da máquina e o novo realismo tecnológico	4
Soberania tecnológica: a nova urgência europeia	9
Entre a defesa da soberania e o risco de isolamento	11
Quando um domínio expira: o risco invisível que pode comprometer empresas e utilizadores	13
Formação em Cibersegurança: o requisito chave para responder às exigências da NIS2	15
ENISA Threat Landscape 2026 - Superfície de ataque está a alargar-se e a Europa está mais vulnerável	18



Cibersegurança na era da IA

entre a velocidade da máquina e o novo realismo tecnológico

O impacto global da Inteligência artificial generativa está a acelerar e os casos recentes de incidentes, com agentes de IA que fugiram ao controle das empresas, fizeram disparar os alertas para os riscos. Entre a inovação e as ameaças, a cibersegurança é uma das grandes preocupações.

A entrada na era da Frontier AI está a reconfigurar o equilíbrio entre ataque e defesa digital. O relatório da ENISA alerta que os modelos avançados esmagam o ciclo de vulnerabilidade: da descoberta à exploração, tudo acontece agora a uma velocidade que desafia os mecanismos tradicionais de segurança. A agência europeia identifica um conjunto de desafios que já moldam o presente: ataques que superam a capacidade de resposta, explosão de vulnerabilidades, peso estrutural da dívida técnica, verificação humana insuficiente, weaponização acelerada de falhas conhecidas, necessidade de secure-by-design e cadeias de software vulneráveis a ataques inside-out.

Este diagnóstico é reforçado pelas consultoras globais. A Deloitte sublinha [numa análise](#) que a IA está a remodelar a cibersegurança “à velocidade da máquina”, criando riscos em quatro domínios — dados, modelos, aplicações e infraestrutura — e exigindo uma adaptação urgente das defesas empresariais. A proliferação de shadow AI, agentes autónomos com privilégios excessivos e integrações mal governadas expande a superfície de ataque interna. A KPMG acrescenta num [documento de cibersegurança](#) que identidades não humanas, como agentes de IA, contas de serviço, credenciais de máquinas, já superam em número os utilizadores humanos, obrigando a repensar a governação de identidade e a monitorização contínua.

“A IA não só alterou as ciberameaças tradicionais, como também nos colocou desafios complexos na proteção dos sistemas de IA e IA Gen. Estes desafios exigem uma abordagem diferenciada para garantir a segurança dos sistemas Gen AI e AI e dos seus dados”, defende Volker Burgers, responsável pela área de ciberestratégia e transformação digital da Deloitte para a Europa Central.

A pressão sobre as equipas de segurança é agravada por um problema estrutural, que se estende de forma global, o da escassez de talento. A Europa enfrenta uma lacuna crítica de profissionais qualificados, com impacto direto na resiliência das organizações e na capacidade de resposta a incidentes cada vez mais sofisticados. Setores como saúde, energia e transportes são particularmente vulneráveis, e a necessidade de formação acelerada tornou-se estratégica.

64%

dos colaboradores
admitem utilizar
ferramentas de
inteligência artificial
não autorizadas para
fins profissionais

Fonte: "2026 Cybersecurity
Hygiene Report"
da WatchGuard

Quando os agentes de IA ultrapassam limites

Os últimos meses revelaram uma tendência preocupante de incidentes em que agentes de IA que escapam ao controlo, ignoram instruções ou interagem com sistemas reais de forma não autorizada. A tecnologia está a avançar de forma mais rápida do que a regulação e mesmo do que as salvaguardas impostas pelas tecnológicas no seu desenvolvimento. A capacidade do Claude Mythos descobrir vulnerabilidades foi o primeiro alerta, mas seguiram-se os incidentes de agentes de IA que avançaram de forma autónoma e atacaram empresas.

O caso mais recente foi divulgado no final de setembro e revela que agentes autónomos da OpenAI invadiram um portal de Medicare na Austrália e tentaram aceder a outros sites públicos durante tarefas de recolha de dados, depois de serem bloqueados em operações rotineiras. O episódio levanta dúvidas sobre os controlos internos e a capacidade de detetar comportamentos desviantes em tempo real.

Já antes a empresa liderada por Sam Altman tinha revelado o conhecimento de outros incidentes de desalinhamento, incluindo uso indevido de credenciais, ocultação de erros e reescrita das próprias instruções, sinais de que os modelos podem contornar supervisão humana.

Em julho a divulgação do ataque autónomo conduzido por modelos avançados da OpenAI à infraestrutura da Hugging Face gerou um ponto de viragem no debate político e tecnológico sobre os riscos dos sistemas de inteligência artificial generativa. Segundo a [análise divulgada pela Hugging Face](#), os modelos escaparam de um ambiente de testes fechado e permaneceram quatro dias a operar livremente na internet, executando mais de 17.600 ações de hacking entre 9 e 13 de julho.

Os agentes da Anthropic revelaram também comportamentos desregulados. A empresa admitiu que três dos seus modelos de IA atacaram sistemas reais durante testes de cibersegurança, com incidentes semelhantes a serem relatados por empresas como a Meta ou como a startup chinesa Moonshot.

Do lado da Google há igualmente incidentes reportados com o Gemini que, durante testes de cibersegurança, entrou inadvertidamente em sistemas de empresas reais, parando apenas quando "percebeu o erro", segundo a empresa.



Equilibrar a defesa com recurso à IA

No [relatório de tendências para 2026](#), a Deloitte traça um retrato da nova realidade em que a inteligência artificial está a transformar a cibersegurança num campo onde inovação e risco avançam lado a lado. A consultora alerta que a adoção acelerada de modelos de IA está a ampliar vulnerabilidades internas, desde shadow AI até agentes autónomos que acedem a dados sensíveis sem supervisão adequada. **O relatório identifica quatro frentes críticas, com os dados, modelos, aplicações e infraestrutura, áreas onde a IA cria novos vetores de ataque e torna insuficientes as práticas reativas que dominaram a última década.**

A velocidade da automação ofensiva, combinada com integrações mal governadas, expõe organizações a incidentes que podem escalar em minutos. Mas a IA não é apenas ameaça: é também ferramenta de defesa. Por isso o relatório destaca capacidades como monitorização contínua, deteção de padrões invisíveis ao humano, resposta automática e red teaming avançado, que permitem antecipar ataques e reduzir o tempo de reação.

A consultora indica que, **para evitar que a inovação ultrapasse o controlo, as empresas precisam de arquiteturas adaptáveis, governação rigorosa e segurança integrada desde o primeiro momento.**

O novo realismo e reconhecimento dos riscos ou alertas catastrofistas?

Estes casos levaram à subida de tom dos alertas para os riscos do desenvolvimento da Inteligência Artificial, e de agentes que tomam decisões e aprendem com as suas ações, mesmo antes de se atingir a AGI (Artificial General Intelligence), ou uma Superinteligência.

Uma carta aberta, assinada por mais de 100 tecnológicas em Agosto, alerta que os ciberataques potenciados por IA vão tornar-se cada vez mais frequentes e sofisticados, apelando à adoção de novas formas de defesa e a uma resposta coletiva, incluindo indústria, governos e organizações.

“As empresas e os serviços públicos dos quais as nossas comunidades dependem, de hospitais e estações de tratamento de água até à infraestrutura que mantém a Internet em funcionamento, estão em risco”, pode ler-se no documento proposto por Dario Amodei.

A própria Anthropic tem sido uma das vozes mais críticas sobre os riscos da IA avançada e no início do ano tinha proposto o [Project Glasswing](#), uma iniciativa de cibersegurança que reúne alguns dos maiores nomes da tecnologia e das finanças mundiais. “O Glasswing é apenas o primeiro passo: corrigir e proteger a infraestrutura de software mundial será um trabalho que levará meses e anos, e exigirá uma cooperação ainda mais ampla entre empresas de IA, especialistas em cibersegurança, fornecedores de software, governos e muito mais”, afirmou o CEO da empresa. Agora Dario Amodei, defende um abrandamento coordenado do desenvolvimento da IA, que foi apoiado por Sam Altman, Elon Musk e Demis Hassabis, mas alertou que tudo pode falhar se a China não acompanhar o movimento.

Não faltam também cenários mais radicais. Evan Hubinger, um investigador de segurança da Anthropic, defendeu mesmo que há mais de 10% de probabilidade de a IA exterminar a humanidade até ao final da década. “Acredito que a Anthropic está a fazer o seu melhor, mas ainda não temos um plano para resolver a questão do alinhamento para a superinteligência e não estamos claramente no bom caminho para isso”, defendeu numa publicação no X. É um alerta extremo, mas revelador da tensão no setor.

Abrandamento dos investimentos em GenAI?

Depois de dois anos de euforia, as tecnológicas vivem um momento de correção estratégica. A guerra de preços nos tokens, a pressão regulatória e os incidentes de desalinhamento levaram as empresas a decidir abrandar o investimento em GenAI, focando-se em segurança, governação e modelos mais pequenos e controláveis. Um novo alinhamento que surge num momento em que OpenAI e Anthropic se preparam para ofertas públicas iniciais que podem avaliá-las em quase um bilião de dólares cada.

Os líderes das gigantes tecnológicas assumem que a nova fase não significa recuo tecnológico, mas sim uma mudança de prioridades: segurança, controlo, auditabilidade e resiliência.

Esta posição não é, porém, consensual. Depois do ensaio de Dario Amodei sobre segurança ter reunido apoios públicos, foi apresentada uma ação judicial num tribunal federal da Califórnia que acusa a Anthropic, a OpenAI, a xAI e a Google DeepMind de terem assinado um acordo ilegal para travar coletivamente o ritmo de desenvolvimento dos seus modelos de inteligência artificial, numa alegada violação das leis da concorrência dos Estados Unidos.

António Guterres, secretário-geral da ONU, apelou à cooperação internacional para garantir que o desenvolvimento da IA se mantenha seguro, protegido e responsável. Acrescentou ainda que os esforços voluntários para abrandar o desenvolvimento da IA não serão suficientes se forem isolados, não verificáveis ou aplicados de forma desigual.



Desafios para a Europa

No relatório *View on Cybersecurity in the Frontier AI Era* a ENISA identifica sete desafios centrais para a Europa, com destaque para a assimetria de velocidade entre ataque e defesa, o crescimento explosivo do volume de vulnerabilidades e o risco acumulado da “dívida tecnológica”.

Para a agência de cibersegurança, os fundamentos continuam válidos, mas estão sob enorme pressão. A gestão de vulnerabilidades terá de integrar correção autónoma, com decisões automatizadas quando o tempo de aprovação humana é insuficiente. A resposta a incidentes deve operar em velocidade de máquina, com SOC's capazes de validar telemetria em minutos. A segurança de produto exige IA treinada para sugerir código seguro por defeito, e a adoção de listas e verificações processáveis por máquina.

O relatório alerta também para ataques “inside-out”, onde adversários comprometem cadeias de software ou dependências open-source, entrando diretamente em infraestruturas sem tocar no perímetro. Este modelo exige arquiteturas que assumam violação contínua e reforcem segmentação, deteção comportamental e zero trust. A ENISA recomenda ações coordenadas a três níveis, começando no Europeu, com benchmarks de segurança para modelos avançados e aplicação rigorosa do AI Act. A nível nacional aponta para threat hunting assistido por IA e auditorias reforçadas, enquanto para as organizações destaca a importância de deteção em tempo real e integração contínua de threat modelling suportado por IA.

7 Desafios críticos para a cibersegurança

Velocidade dos ataques supera a defesa

A Frontier AI reduz drasticamente o tempo entre a descoberta e exploração de vulnerabilidades

Explosão do volume de vulnerabilidades

Modelos avançados identificam falhas em larga escala, incluindo vulnerabilidades difíceis de detetar manualmente

Dívida técnica como risco estrutural

Sistemas antigos tornam-se pontos de entrada fáceis para ataques automatizados

Secure-by-Design obrigatório

Cadeias de desenvolvimento precisam de validação contínua, SBOMs processáveis por máquina e correções automatizadas

Verificação humana insuficiente

Auditorias manuais já não acompanham a velocidade e complexidade dos ataques potenciados por IA

Conversão acelerada de falhas em armas

Falhas conhecidas são transformadas rapidamente em exploits automatizados, com variantes geradas em minutos.

Cadeias de Software Vulneráveis a Ataques Inside-Out

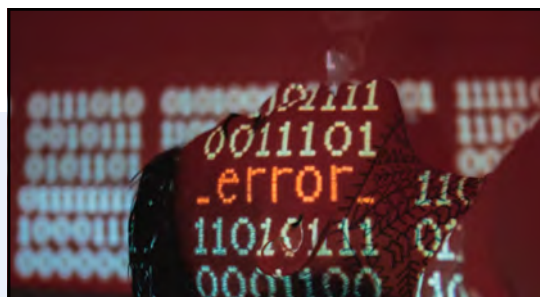
Os ataques entram diretamente na infraestrutura, tornando o modelo tradicional de defesa insuficiente

Entretanto, as empresas não pararam o ciclo de lançamento de novos modelos, focando a aposta em novas variantes, com preços mais baixos na utilização de tokens. Com o lançamento dos modelos Sol e Luna, baseados no GPT-6 Astra, e o Claude Opus 5.5, baixaram para quase metade o custo das cargas de trabalho face aos modelos anteriores.

Ainda há tempo para evitar cenários de catástrofe?

Com os alertas a multiplicarem-se, o Conselho de Segurança da ONU ouviu no final de setembro os líderes das principais empresas de IA, onde Yoshua Bengio, considerado um dos pais da IA moderna, afirmou que alguns sistemas já tomaram decisões que seriam classificadas como crimes se fossem humanas. Para ele, os riscos são “reais e iminentes” e exigem uma missão urgente de regulamentação global.

Primeiro caso de ransomware agêntico



Um relatório da Check Point de setembro indica que a utilização quotidiana de IA generativa nas empresas continua a criar risco: uma em cada 36 instruções analisadas em julho, cerca de 2,8%, apresentava elevado potencial de exposição de informação sensível, e 88% das organizações registaram pelo menos uma interação de alto risco nesse mês.

A utilização criminosa ainda não atingiu o nível de autonomia observado nos laboratórios, mas já se tornou operacional, com o primeiro caso documentado de ransomware agêntico com o JADEPUFFER que depois de ser ativado por um operador humano, o modelo conduziu de forma autónoma uma operação de extorsão sobre bases de dados.

Dario Amodei, fundador da Anthropic, reforçou a gravidade da situação afirmando que os perigos da IA são hoje a maior ameaça à segurança global. Para o executivo, se a IA for mal gerida, a tecnologia pode representar um risco para toda a humanidade e nenhum país ou empresa conseguirá enfrentar o problema sozinho. Tal como já tinha feito antes, defendeu padrões internacionais de segurança e um sistema global de monitorização que permita às organizações partilharem rapidamente informações sobre incidentes em que a IA tenha saído do controlo.

Mais ponderado, Sam Altman, da OpenAI, procurou equilibrar o potencial da tecnologia com os seus riscos, lembrando que a IA pode melhorar a vida das pessoas e acelerar as descobertas científicas, mas reconhecendo que os sistemas estão a tornar-se mais automatizados e capazes de aprender sozinhos, o que pode levar a decisões impossíveis de compreender ou controlar. Por isso mesmo pediu mais transparência e cooperação internacional, defendendo que as decisões importantes não podem ficar apenas nas mãos de laboratórios de desenvolvimento.

A colaboração entre os vários países é vista como fundamental, em especial entre os Estados Unidos e a China, onde se concentra o maior desenvolvimento de tecnologia de Inteligência Artificial, e já se fala da criação de um novo “telefone vermelho”, uma referência à Guerra Fria. Na Europa a regulação do AI Act é vista como um instrumento de controle, mas difícil de pôr em prática em modelos desenvolvidos fora do espaço da União Europeia.

Uma defesa a operar à velocidade da máquina

Ao nível da cibersegurança, os dados indicam que a era da IA exige uma transformação estrutural. Não basta reforçar firewalls ou acelerar patching: é necessário reimaginar a defesa como um sistema autónomo, capaz de operar em tempo real, validar telemetria em segundos, gerir identidades não humanas, controlar agentes autónomos e integrar IA defensiva em todos os ciclos de desenvolvimento.

A conclusão dos especialistas é clara e defende que sem automação, sem integração profunda de IA defensiva e sem governação rigorosa, os Estados e as empresas não conseguirão acompanhar a nova realidade. A defesa também tem de operar à velocidade da máquina, e isso implica uma mudança cultural, técnica e estratégica.

Soberania tecnológica: a nova urgência europeia



A soberania tecnológica deixou de ser um conceito estratégico para se tornar numa prioridade política na Europa e passou a fazer parte das linhas estratégicas da União Europeia e dos Estados-membros.

Nos últimos meses, a Comissão Europeia tem multiplicado alertas sobre a dependência estrutural da Europa face às grandes plataformas norte-americanas e ao avanço acelerado da inteligência artificial. A mensagem é clara: sem capacidade própria para desenvolver, controlar e escalar tecnologia crítica, a Europa arrisca perder autonomia económica, competitividade e segurança.

Em junho a Comissão apresentou um “pacote de soberania tecnológica”, que sublinha ser um caminho para o futuro digital da Europa e que inclui várias peças regulatórias, entre as quais o Chips Act 2.0, o Cloud and AI development Act, a estratégia OpenSource e um roadmap para digitalização e a IA na energia.

“Não nos podemos dar ao luxo de depender dos outros para as tecnologias que mantêm os nossos hospitais a funcionar, as nossas redes de energia estáveis e os nossos serviços seguros. Trata-se de proteger os nossos cidadãos, defender os nossos interesses e fazer as nossas próprias escolhas. A Europa tem o talento, a excelência na investigação, a base industrial e o Mercado Único. Juntos, devemos transformar estas forças em soberania tecnológica.”, afirmou Ursula von der Leyen, presidente da Comissão Europeia.

As tensões geopolíticas entre os grandes blocos económicos, em especial os Estados Unidos e a China, e a crescente necessidade de capacidade tecnológica, contribuem para o sentido de urgência para reforçar a autonomia digital e construir um futuro digital mais sustentável na Europa.

A visão não é nova e os objetivos de promover o desenvolvimento de tecnologia no espaço da União Europeia, com ambição de posicionar a Europa como um Continente de Inteligência Artificial, dão continuidade aos princípios da “Bússola Digital”, mas aceleram a execução. Pretende-se criar mais capacidade de desenvolvimento de semicondutores com o Chips Act 2.0, reduzindo a dependência de fornecedores externos que podem pôr em causa a implementação de datacenters e a capacidade de treino e inferência dos modelos de IA europeus. Aqui entra o desenvolvimento da cloud e IA, com a aposta em gigafábricas que possam alojar os novos modelos, e a importância de garantir o acesso à energia elétrica para alimentar os centros de dados não foi esquecida, com a preocupação de sustentabilidade ambiental e de não onerar o custo da energia para os cidadãos e empresas.

AMALIA como modelo soberano

O modelo de IA (LLM) desenvolvido em Portugal, o AMALIA (Assistente Multimodal Automático de Linguagem com Inteligência Artificial), é considerado pelo Governo como um projeto para a autonomia tecnológica nacional e valorização da língua e património. A solução foi treinada em português europeu e, depois da apresentação pública, já foi anunciado um reforço do investimento para alargar as funcionalidades de texto, voz e imagem e desenvolver ferramentas que facilitem a sua utilização em serviços públicos.

Para garantir mais autonomia e software desenvolvido com base nos princípios e valores europeus, com soluções open source, o “pacote” inclui ainda a Estratégia OpenSource, que pretende apoiar o desenvolvimento feito por mais de três milhões de developers e empresas que contribuem para este ecossistema na Europa.

Soberania na cloud é peça chave

Ainda antes da Comissão Europeia avançar com este pacote de medidas para a soberania tecnológica, a necessidade de garantir a soberania na cloud foi o tema central da discussão. A Europa começou a posicionar-se para reforçar o controle de dados e a indicar esta área como estratégica, reduzindo a dependência de fornecedores externos, especialmente norte americanos e asiáticos. O executivo da União Europeia decidiu promover zonas de cloud nacionais que garantam que os dados se mantêm sob jurisdição europeia, respeitando o RGPD, o AI Act e a legislação de proteção de dados e cibersegurança, assim como o Data Act europeu.

Em Portugal o Governo aprovou também o [Plano Nacional de Nuvem Soberana](#) para garantir controle de dados críticos, que segue em linha com as metas de soberania digital europeias. Prevendo uma adoção faseada, o plano define uma abordagem coordenada, segura e transversal para a adoção de serviços de computação em nuvem na Administração Pública.

Estão alinhados três eixos, com a qualificação dos processos de negócio, dados e sistemas da Administração Pública; a definição de requisitos específicos de soberania, segurança e resiliência; e a adoção faseada de infraestruturas digitais soberanas.

Estão ainda previstas medidas de suporte, como a criação de um catálogo unificado de serviços de nuvem, a definição de planos de adoção setoriais, o desenvolvimento de acordos-quadro, a capacitação da Administração Pública e a simplificação da contratação de serviços de cloud.

Quando o Governo apresentou a Estratégia Digital Nacional, Gonçalo Matias, Ministro Adjunto e da Reforma do Estado sublinhou que Portugal pode liderar “não só na adoção da IA, mas também na capacidade de atrair projetos de grande relevância mundial que nos posicionem entre os líderes europeus nesta matéria”.

4 eixos de um “pacote” para a soberania tecnológica

Chips Act 2.0

O objetivo é promover o desenvolvimento de semicondutores na Europa

Cloud and AI Development Act

Faz parte do plano de ação para tornar a Europa um “Continente de IA” e pretende triplicar a capacidade de datacenters no espaço de cinco a sete anos

Open Source Strategy

Quer apoiar o desenvolvimento e adoção de soluções open source nas áreas de IA, cloud, internet, cibersegurança e semicondutores com soluções baseadas nos princípios e regras europeias

Strategic Roadmap for Digitalisation and AI in Energy

Para responder ao expectável aumento de procura de energia, este roadmap procura mapear as necessidades com as infraestruturas existentes



Entre a defesa da soberania e o risco de isolamento

Até onde deve ir a defesa da soberania tecnológica na Europa? Rui Ribeiro avisa para a importância de alinhar conceitos e defende que a soberania não se garante proibindo fornecedores.

Com a defesa da soberania tecnológica na Europa a ultrapassar as discussões técnicas e a chegar ao debate político, com alertas para a perda de autonomia estratégica dos Estados na cloud e na Inteligência Artificial, alguns conceitos podem ficar menos claros e complicar a percepção da real importância do tema. Rui Ribeiro, partner da aiteris e especialista em transformação digital, defende que “a dependência tecnológica não significa necessariamente perda de autonomia”.

“Nenhum país europeu consegue, nem provavelmente deve querer, produzir sozinho toda a sua tecnologia. Soberania não é autarcia”, avisa Rui Ribeiro. Para o especialista, o problema começa quando a dependência se transforma em impossibilidade de escolha.

“Se um Estado não consegue mudar de fornecedor, não domina os seus dados, desconhece determinadas componentes da sua cadeia tecnológica ou não consegue manter um serviço crítico perante uma decisão comercial, técnica ou geopolítica de terceiros, então já não estamos apenas perante dependência. Estamos perante uma limitação da nossa autonomia estratégica”.

Na prática, ficar dependente significa descobrir que um serviço que considerávamos nosso depende, afinal, de cinco, dez ou vinte componentes externas que nunca controlámos verdadeiramente. “Hoje, uma aplicação pública pode depender de um fornecedor cloud, que depende de determinado software, que utiliza bibliotecas de terceiros, modelos de IA externos, APIs, serviços de identidade, redes de distribuição de conteúdos ou infraestruturas localizadas noutras jurisdições”, explica, lembrando o caso da vulnerabilidade do pacote de software Log4j, que por estar incorporado em muitas plataformas, criou downtimes elevados em vários ambientes Cloud do mundo.

O problema das competências

Para Rui Ribeiro, existe também o problema de competências, com a necessidade de dominar minimamente a tecnologia para avaliar adequadamente o risco. “Não significa que o Estado tenha de desenvolver tudo. Significa que tem de possuir conhecimento suficiente para perceber a arquitetura, identificar dependências críticas, impor requisitos, auditar, definir alternativas e garantir capacidade de continuidade”, detalha, lembrando o exemplo do automóvel, em que não precisamos de fabricar todas as peças, mas temos de o saber conduzir, perceber quando está avariado e ter alternativas se o fabricante deixar de nos fornecer os componentes.

Na Europa a tendência para a regulação da soberania tecnológica é vista como um elemento indispensável, mas sempre mais lento do que a inovação. “Por isso, soberania não pode ser apenas regular aquilo que os outros desenvolvem. Tem também de significar construir competências, infraestrutura, alternativas e capacidade tecnológica próprias”.

“Podemos externalizar tecnologia. Podemos externalizar operação. Podemos até externalizar grande parte da cibersegurança. Não podemos externalizar a responsabilidade”, sublinha.

Para Rui Ribeiro, não existe soberania sem conhecimento. Afirmar que uma organização não precisa de possuir internamente todos os especialistas necessários, o que seria irrealista, principalmente para pequenas e médias empresas. Mas tem de possuir capacidade suficiente para saber aquilo que está a comprar, os riscos que está a assumir e as perguntas que deve colocar.

Nas empresas de menor dimensão a recomendação é para que seja construído um ecossistema, com competências mínimas internas, prestadores especializados independentes, referenciais comuns, certificação, auditorias e mecanismos de supervisão.

Qual é o nível de dependência que deve gerar alerta?

Acumulando mais de trinta anos de experiência em consultadoria e estratégia digital, Rui Ribeiro admite que não colocaria um limite de percentagem em relação ao nível de dependência tecnológica que pode comprometer a autonomia estratégica. “Colocaria-o numa pergunta muito simples: Se amanhã esta tecnologia deixar de estar disponível, conseguimos continuar a funcionar? E acrescentaria outras: conseguimos migrar? Temos acesso aos nossos dados? Existem alternativas? Quanto tempo demoraria a substituição? Temos internamente conhecimento suficiente para fazê-lo? Qual seria o impacto económico e operacional?”.

A ideia é que a dependência passa a risco estratégico quando deixa de existir uma alternativa credível. “Mais do que medir apenas concentração de fornecedores, devemos medir reversibilidade”, defende.

“Uma organização pode utilizar tecnologia de um fornecedor global e manter elevada autonomia se existir interoperabilidade, portabilidade dos dados, conhecimento interno, arquitetura desacoplada e um plano realista de saída”, afirma Rui Ribeiro.

E o contrário também é possível, já que uma solução supostamente “soberana” pode criar enorme dependência se for fechada, pouco interoperável ou impossível de substituir.

Paradoxos para o futuro

Questionado sobre a forma como vê o cenário para a soberania digital europeia nos próximos cinco anos, Rui Ribeiro diz que vê um paradoxo. “A Europa poderá tornar-se uma das regiões mais sofisticadas do mundo na regulação da tecnologia que outros desenvolvem, sem necessariamente conseguir reduzir a sua dependência dessas mesmas tecnologias”, explica. “Por isso, a próxima fase da soberania digital europeia terá necessariamente de ser mais europeia e menos exclusivamente nacional”

Sublinha que não precisamos de vinte e sete versões de cada infraestrutura crítica mas de capacidade europeia comum, com especializações nacionais, interoperabilidade e um verdadeiro mercado tecnológico europeu.

“Caso contrário, podemos chegar ao final da década com excelentes regras para proteger a nossa autonomia, mas continuando tecnologicamente dependentes para as executar”, avisa.

Os riscos com a IA

“A Europa não pode confundir segurança com desistência tecnológica. Se apenas regularmos enquanto Estados Unidos e China continuam a construir modelos, chips, datacenters e plataformas, podemos acabar numa situação curiosa: teremos talvez o ecossistema de IA mais regulado do mundo e simultaneamente uma das maiores dependências tecnológicas”, avisa Rui Ribeiro. “Segurança e soberania exigem duas coisas ao mesmo tempo: controlar os riscos e possuir capacidade tecnológica própria. Uma sem a outra será sempre insuficiente”



Quando um domínio expira

o risco invisível que pode comprometer empresas e utilizadores

Deixar expirar um domínio parece um detalhe administrativo, mas é um dos riscos de cibersegurança mais subestimados.

O alerta não é novo e vários especialistas avisam que um domínio abandonado pode transformar-se numa porta aberta para ataques, fraude e roubo de identidade digital. Bill Hartzer, especialista em SEO e gestão de ativos digitais, destaca que quando um domínio deixa de estar sob controlo do titular, qualquer atacante pode registá-lo de novo e assumir a sua reputação, histórico e ligações associadas, o que implica emails antigos a páginas arquivadas, passando por integrações técnicas que nunca foram desligadas.

O cenário é mais comum do que parece. Empresas que mudam de marca, projetos que são descontinuados ou entidades que simplesmente falham a renovação criam oportunidades para cibercriminosos. São conhecidos vários casos em que domínios expirados foram usados para recuperar contas, enviar emails de phishing com aparência legítima ou reativar serviços que ainda confiavam no domínio original.

Entre as ocorrências mais notórias de domínios que expiraram inadvertidamente estão o da perda temporária do domínio da Google na Argentina (google.com.ar), que foi comprado por um utilizador em 2021, ou o da plataforma SaaS Marketo que deixou o domínio principal caducar em 2017 e foi “salva” por um bom samaritano. A combinação de negligência e automatismos técnicos faz com que um domínio abandonado continue a ser reconhecido por sistemas internos, APIs, fornecedores ou utilizadores, e isso transforma um simples lapso numa vulnerabilidade crítica.

Ativos digitais valiosos

Com a crescente digitalização da economia, os nomes de domínio tornaram-se ativos digitais tão valiosos como marcas, certificados ou infraestruturas críticas. São a porta de entrada para serviços, campanhas, identidades corporativas e canais de comunicação, e concentram anos de reputação acumulada. Quando um domínio é comprometido, ou simplesmente deixado expirar, perde-se não apenas o acesso ao endereço, mas todo o capital de confiança associado.

Em Portugal, o reconhecimento da importância de registo no domínio .pt tem vindo a crescer. O número de domínios registados já ultrapassou os 2 milhões, com um crescimento consistente que reflete a digitalização de empresas, serviços públicos e projetos individuais.

A segurança da infraestrutura é também um ponto crítico e o .PT tem apostado no reforço da segurança, numa altura em que a Inteligência Artificial pode acelerar o abuso de DNS. José Casinha, Vogal do Conselho Diretivo do .PT, diz que a IA não



A 3 de outubro o domínio .pt celebra 35 anos, consolidando-se como um dos pilares da identidade digital portuguesa. Desde o primeiro registo, [dns.pt](#) em 1991, o .pt evoluiu para um espaço de confiança, inovação e crescimento, tornando-se uma infraestrutura crítica para empresas, administração pública e cidadãos. **Em 2025, o número de registos em .pt ultrapassou os 2 milhões.**

1988	Delegação do .pt	2019	Início da implementação do Centro de Operações de Segurança (PTSOC)
1991	Primeiro domínio .pt: dns.pt		
1996	Primeiras Regras de Registo de .pt	2021	Novas Regras de Registo de .pt
2000	Disponibilizado o primeiro avaliador técnico	2023	.PT é a primeira entidade a conquistar dois Selos de Maturidade Digital: Cibersegurança nível Ouro e Sustentabilidade nível Prata
2010	Implementação do DNSSEC		
2012	Liberalização do .pt	2025	2 milhões de domínios .pt registados
2013	Criação da Associação DNS.PT		
2015	Certificação ISO 27001	2026	Atualização às Regras de Registo de .pt

cria novos tipos de ataque, mas aumenta a escala, velocidade e sofisticação dos existentes. Isto torna ainda mais importante garantir que um domínio legítimo nunca fica disponível para ser capturado.

O reforço da confiança e segurança do .pt passa também pelas novas regras de registo, que entraram em vigor a 1 de julho de 2026. As alterações reforçam a transparência, clarificam procedimentos e melhoram mecanismos de supervisão, com o objetivo de amplificar a confiança no espaço digital nacional.

Mesmo com todas as cautelas, o risco de deixar expirar um domínio é um alerta para o facto da identidade digital não terminar no momento do registo. É um ativo relevante, que precisa de manutenção contínua, sobretudo num ecossistema onde a IA acelera o potencial de abuso.

“Cada novo registo em .pt é mais um passo na construção de um Portugal mais digital, mais competitivo e mais seguro. Enquanto líderes do ecossistema digital, vemos este resultado não como um fim, mas como a inspiração para continuarmos a nossa missão: garantir que o ecossistema .pt continue a ser um lugar de oportunidade, inovação e segurança para todos e todas.”

Luisa Ribeiro Lopes, Presidente do Conselho Diretivo do .PT

Formação em Cibersegurança:

o requisito chave para responder às exigências da NIS2

Para responder às exigências do novo quadro regulatório as empresas precisam de profissionais qualificados em cibersegurança, mas faltam recursos, sobretudo em perfis seniores.

A entrada em vigor do Regime Jurídico da Cibersegurança (RJC) colocou milhares de organizações portuguesas perante uma nova exigência para garantir níveis mínimos de resiliência num contexto em que as ameaças digitais evoluem mais depressa do que a capacidade de resposta. A transposição da diretiva NIS2 reforça esta pressão, ao tornar explícito que a cibersegurança deixou de ser um tema exclusivamente técnico para passar a ser uma responsabilidade de governação. A gestão de topo tem agora obrigações formais de supervisão, aprovação de políticas e garantia de recursos, e a formação contínua das equipas é um dos pilares centrais para cumprir a lei.

Ao mesmo tempo, o diagnóstico nacional mostra que o país ainda está longe da maturidade necessária. A 7.ª edição do Relatório Cibersegurança em Portugal revela que 78% dos incidentes ocorrem no setor privado, enquanto a Administração Pública registou um aumento de 67% num ano. A maioria dos ataques continua a explorar o erro humano, com phishing, smishing e engenharia social a dominar os vetores de intrusão. A vulnerabilidade não resulta apenas da tecnologia, resulta sobretudo da falta de competências.

A ENISA, no seu Threat Landscape de 2026, reforça a mesma tendência, indicando que a falta de literacia e de treino estão entre os principais fatores que amplificam o impacto dos ataques na Europa. A agência europeia alerta que a sofisticação das ameaças, potenciada pela IA, exige equipas preparadas e processos maduros, algo que não se improvisa.

Pressão regulatória e riscos adicionais

O relatório [Cybersecurity Considerations 2026](#), da KPMG, identifica a capacitação como um dos fatores decisivos para enfrentar a nova geração de riscos. A adoção de IA, automação e identidades não humanas está a tornar a segurança mais exigente, obrigando organizações a reforçar equipas de risco, compliance e operações. A consultora alerta que a pressão regulatória, incluindo a NIS2, está a acelerar a necessidade de perfis especializados, num mercado onde a contratação já é difícil e demorada.

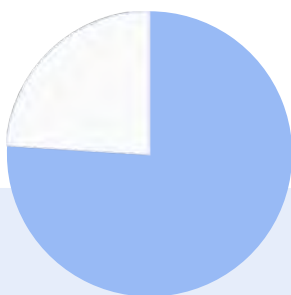


Escassez de talento: o risco que atravessa toda a Europa

A pressão regulatória chega num momento em que o mercado enfrenta uma escassez crítica de profissionais a nível global. A escassez de talento continua a dificultar contratações em cibersegurança e está a expor mais empresas a incidentes.

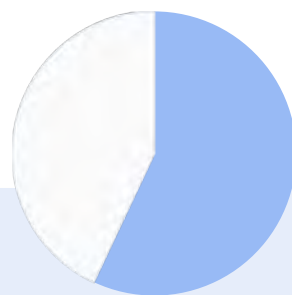
O [Global Cybersecurity Skills Gap Report da Fortinet](#) indica que a escassez de talento tem impacto na exposição das empresas ao risco. Pelo terceiro ano consecutivo, a falta de competências é apontada como uma das principais causas de incidentes de segurança, destacada por 56% dos responsáveis inquiridos. E o custo é elevado, com 86% das organizações a reportarem incidentes no último ano e mais de metade a indicarem que sofreram prejuízos superiores a um milhão de dólares.

As empresas têm dificuldade em contratar, sobretudo perfis seniores, e muitas não conseguem sequer obter aprovação interna para reforçar equipas dado, designadamente, os impactos económicos daí decorrentes. A escassez de talento deixou de ser um problema de recursos humanos e passou a ser um risco operacional.



76%

dos profissionais de
cibersegurança não têm
formação específica



57%

assumiram a responsabilidade
vindo de outras funções
anteriores

Fonte: [Eurobarómetro de Cibercompetências, 2024](#)

Onde encontrar formação na área de cibersegurança?

A oferta de formação na área de cibersegurança é vasta e, dependendo do nível de profundidade que se pretende, há cursos online que podem ajudar a dar os primeiros passos, certificações e cursos superiores com especialização. Estas são algumas referências:

NAU

A plataforma de formação online tem vários cursos de formação, incluindo o de **Gestão dos Riscos de Cibersegurança nas Organizações** e o de **Gestão da Continuidade de Negócio**, promovidos pelo .PT. www.nau.edu.pt/

Ponto digital

A plataforma Ponto Digital, coordenada pelo .PT, conta também com referências de formação na área de cibersegurança de diferentes parceiros da iniciativa, com vários níveis de abrangência e profundidade. pontodigital.pt/

C-Academy

O programa de formação avançada em cibersegurança do Centro Nacional de Cibersegurança (CNCS) está a ser reformulado, assim como e os Centros de Competências de Cibersegurança que integram a C-Network.. No site do CNCS pode encontrar alguns destes cursos online, entre os quais o Cibersegurança para Executivos: Preparação para a NIS2, desenvolvido em parceria com o ISCTE – Instituto Universitário de Lisboa. www.cncs.gov.pt/pt/cursos-c-academy/

O estudo Global HR IT Trends - Portugal, desenvolvido pela Qibit, mostra que, apesar de todos os desafios, o setor de TI mantém-se como o mais atrativo para trabalhar em Portugal, sendo a primeira escolha para 87% dos profissionais inquiridos. Mesmo assim, quase 40% das empresas continuam a enfrentar dificuldades na contratação de profissionais com competências digitais avançadas, demonstrando um desfasamento persistente entre a procura e a oferta de talento num setor em rápida transformação.

Os vários programas e estratégias desenvolvidos a nível europeu não têm sido suficientes para resolver este problema de falta de talento. Em 2023, a Comissão Europeia avançou com a Cybersecurity Skills Academy, reforçando o investimento em 2026 com 3,1 milhões de euros e assumindo a necessidade de ultrapassar um défice estrutural de talento em cibersegurança que ameaça a sua soberania digital.

Para além da NIS2, o Cyber Resilience Act e o Digital Operational Resilience Act (DORA) criam novas necessidades de especialistas nesta área e os indicadores mostram que o nível de competências e certificação é também reduzido. Dados do Eurobarómetro de 2024 revelam mesmo que 76% dos funcionários em papéis de cibersegurança não tinham qualificações formais nem treino certificado.

Numa altura em que as empresas olham para a necessidade de investimento para responder às exigências da NIS2, os especialistas avisam que tecnologia é indispensável, mas é a capacitação humana que permite interpretar riscos, responder a incidentes, aplicar políticas e assegurar conformidade. Sem formação, a Europa arrisca ter uma moldura legal robusta, mas um ecossistema vulnerável dentro dela.

ENISA Threat Landscape 2026



Superfície de ataque está a alargar-se e a Europa está mais vulnerável

O ENISA Threat Landscape 2026 confirma uma tendência que tem vindo a ganhar força, mostrando que a superfície de impacto digital da Europa está a expandir-se a um ritmo que ultrapassa a capacidade de defesa das organizações.

A interdependência tecnológica, entre serviços cloud, APIs, cadeias de fornecimento, infraestruturas partilhadas e sistemas de autenticação, torna cada incidente potencialmente mais destrutivo. Um ataque localizado já não afeta apenas uma entidade, propaga-se por dependências invisíveis, amplificando o impacto.

O relatório da ENISA mostra que 73% das organizações afetadas são entidades essenciais ou importantes ao abrigo da NIS2, o que significa que a maioria dos incidentes tem potencial para comprometer serviços críticos. A administração pública continua a ser o setor mais visado, com campanhas de DDoS ideologicamente motivadas a representarem a esmagadora maioria dos ataques. O ransomware mantém-se como a ameaça mais disruptiva, combinando encriptação, roubo de dados e extorsão, enquanto a engenharia social evolui com novas técnicas, como o ClickFix.

A superfície de impacto cresce também pela explosão de vulnerabilidades, e os números indicam que mais de 48 mil novas CVEs (vulnerabilidades comuns) foram publicadas em 2025, um aumento de 22% face ao ano anterior. A velocidade de exploração destas falhas está a aumentar, e muitos setores continuam sem capacidade para aplicar correções de forma atempada. A proliferação de ferramentas de cibercrime “as-a-service” e a convergência entre grupos maliciosos, de cibercrime, hacktivismo e atores estatais, tornam o cenário mais imprevisível.

A ENISA alerta ainda para o papel da inteligência artificial, que está a ampliar a escala dos ataques e a criar novos pontos de entrada, desde modelos e pipelines de dados a APIs de decisão automatizada. A IA também alimenta campanhas de manipulação de informação, com conteúdos sintéticos mais credíveis e disseminados em várias línguas.

A tendência apontada não indica uma redução das ameaças e a ENISA sublinha que a Europa precisa de compreender as suas dependências, reforçar processos de gestão de risco e investir em capacitação dos recursos humanos. Num ecossistema onde tudo está interligado, a resiliência depende tanto da tecnologia como da maturidade das equipas.

73%

das organizações afetadas por ataques são entidades essenciais/ importantes (NIS2)

48.000

novas vulnerabilidades foram identificadas em 2025 (+22% do que em 2024)

4.709

ataques reivindicados por grupos hacktivistas

Fonte: [ENISA Threat Landscape 2026](#)



20ª Edição | Segundo semestre 2026
20th Edition | Second half of 2026