Conselho
da União Europeia

Bruxelas, 9 de julho de 2026
(OR. en)

11711/26

CYBER 337
JAI 979
TELECOM 383
CSC 483
DATAPROTECT 234
RELEX 990
COSI 111
COPS 434

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	8 de julho de 2026
para:	Thérèse BLANCHET, secretária-geral do Conselho da União Europeia
n.° doc. Com.:	COM(2026) 577 final
Assunto:	COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES Plano de Ação para a Cibersegurança e a Inteligência Artificial

Envia-se em anexo, à atenção das delegações, o documento COM(2026) 577 final.

Anexo: COM(2026) 577 final

COMISSÃO
EUROPEIA

Estrasburgo, 7.7.2026
COM(2026) 577 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES

Plano de Ação para a Cibersegurança e a Inteligência Artificial

1. Introdução

A inteligência artificial (IA) de fronteira assinala uma mudança na cibersegurança. Os modelos de IA de fronteira (ou seja, os modelos de IA mais avançados disponíveis ou em desenvolvimento) proporcionam capacidades acrescidas para reforçar a preparação e melhorar a deteção e a resposta a ameaças, criando **oportunidades sem precedentes para aumentar a ciber-resiliência**. À medida que estas capacidades continuam a evoluir[1], a IA permitirá que as equipas de cibersegurança atuem mais rapidamente e em maior escala, capacitando as organizações para enfrentar ameaças emergentes de forma mais eficaz. Ao mesmo tempo, as **capacidades avançadas da IA disponíveis atualmente**, nomeadamente através de fonte aberta, **já podem ser utilizadas para reforçar a ciber-resiliência da UE**[2].

A IA já se tornou **um elemento determinante no panorama das ameaças**, permitindo ciberoperações mais automatizadas, moduláveis e sofisticadas, incluindo atividades de cibercriminalidade[3]. Embora as capacidades a nível de fronteira estejam atualmente concentradas num pequeno número de modelos e sistemas de IA (ou seja, modelos e sistemas que conseguem desempenhar uma grande variedade de tarefas e que se aproximam, atingem ou excedem o atual estado da arte)[4], o défice de capacidades está a diminuir à medida que os modelos de fonte aberta continuam a melhorar. Consequentemente, prevê-se que as capacidades reais de fronteira se tornem cada vez mais acessíveis ao longo do tempo, nomeadamente a intervenientes mal-intencionados, como os cibercriminosos, que podem explorar essas capacidades para executar ataques mais complexos.

A UE está a entrar preparada neste novo paradigma. Nos últimos anos, criou os princípios fundamentais: as bases jurídicas e operacionais para abordar a cibersegurança na era da IA. O **Regulamento IA** estabelece o primeiro quadro juridicamente vinculativo do mundo para gerir os riscos decorrentes dos sistemas e modelos de IA, nomeadamente os riscos sistémicos dos modelos de IA de finalidade geral mais avançados, como os riscos de utilização abusiva do ciberespaço[5]. O **Regulamento de Ciber-Resiliência** (que ficará plenamente aplicável até ao final de 2027) visa a segurança das cadeias de abastecimento, impondo a segurança desde a conceção e a gestão das vulnerabilidades ao longo de todo o ciclo de vida dos produtos de *software* e *hardware* no mercado da UE[6]. Em conjunto, o Regulamento IA e o Regulamento de Ciber-Resiliência ajudam a garantir que os modelos e sistemas de IA e os produtos com elementos digitais são construídos e mantidos tendo em mente a segurança. Paralelamente, a **Diretiva SRI 2**[7], juntamente com o **Regulamento Resiliência Operacional Digital**[8] para o setor financeiro, estabelece um quadro baseado no risco para a cibersegurança de setores

---

[1] Estudos recentes do Instituto de Segurança de IA do Reino Unido (AISI) sugerem que, em testes de cibersegurança controlados, os modelos de IA mais avançados são capazes de concluir tarefas cada vez mais extensas sem ajuda humana. A duração estimada das tarefas que conseguem desempenhar tem duplicado ao longo de meses, e não de anos, e os resultados recentes sugerem que este ritmo pode estar a acelerar.

[2] *AI is changing the economics of vulnerability discovery. Defenders should adapt now*, CERT-UE, abril de 2026.

[3] ENISA, *ENISA Threat landscape 2025*[não traduzido para português], outubro de 2025.

[4] Tal como definido no artigo 2.º, ponto 4, da proposta de ato legislativo sobre o desenvolvimento da nuvem e da IA, COM(2026) 502 final.

[5] Regulamento (UE) 2024/1689.

[6] Regulamento (UE) 2024/2847.

[7] Diretiva (UE) 2022/2555, que abrange 11 setores de importância crítica (energia, transportes, setor bancário, infraestruturas do mercado financeiro, saúde, água potável, águas residuais, infraestruturas digitais, gestão de serviços TIC, administração pública e espaço) e sete outros setores críticos (serviços postais e de estafeta; gestão de resíduos; produção, fabrico e distribuição de produtos químicos; produção, transformação e distribuição de produtos alimentares; indústria transformadora; prestadores de serviços digitais; e investigação).

[8] Regulamento (UE) 2022/2554.

críticos. Estes atos legislativos estabelecem um quadro sólido que, se aplicado de forma eficaz, é robusto à luz da evolução tecnológica e das ameaças. O **Regulamento de Cibersolidariedade** complementa este quadro com mecanismos operacionais para apoiar os Estados-Membros na preparação, deteção e resposta a incidentes significativos e em grande escala[9]. Em conjunto, estas medidas contribuem para os objetivos da **Estratégia para uma União da Preparação**[10] e da **Estratégia Europeia de Segurança Interna**[11].

As cibercapacidades avançadas baseadas na IA são também um ativo fundamental para garantir a segurança da nossa União. Embora estas capacidades, disponíveis através de diferentes modelos, incluindo os abertos, já possam reforçar a ciber-resiliência da UE, as capacidades de fronteira são desenvolvidas sobretudo fora da UE e a sua disponibilidade é frequentemente determinada por processos pouco transparentes e conduzidos por países terceiros. Por conseguinte, o conhecimento destas capacidades e o acesso às mesmas são uma questão não só de resiliência digital, mas também de soberania tecnológica da Europa. Para preservar esta soberania, a UE deve assegurar que a adoção de capacidades avançadas de cibersegurança baseadas na IA não crie novas dependências estratégicas. Ao mesmo tempo, a Europa deve intensificar a sua resiliência para acompanhar este panorama de ameaças em rápida evolução.

A UE já tomou **medidas estratégicas no sentido de reduzir as dependências de tecnologias críticas e aumentar as capacidades internas**. Por meio dos programas Horizonte Europa e Europa Digital, a UE já está a financiar o desenvolvimento de cibercapacidades avançadas baseadas na IA e o Fundo do Conselho Europeu da Inovação tornou-se um importante investidor em tecnologia profunda na Europa, incluindo investimentos em cibersegurança e em empresas em fase de arranque e em fase de expansão no domínio da tecnologia de IA[12]. Além disso, o **ato legislativo sobre o desenvolvimento da nuvem e da IA**[13], recentemente proposto, alargará a capacidade dos centros de dados da UE e a autonomia da computação em nuvem e da IA, apoiando uma implantação mais ampla da IA — incluindo ferramentas e aplicações relacionadas com o ciberespaço. Permitirá à UE recorrer a capacidades críticas de computação em nuvem e de IA, reduzindo assim as dependências perante riscos geopolíticos e de segurança. A proposta baseia-se na **Estratégia de Aplicação da IA** e no **Plano de Ação para um Continente da IA**, reconhecendo, nomeadamente, a necessidade de lançar grandes desafios para apoiar e expandir a IA de fronteira.

Alicerçada nestas bases sólidas, **a UE deve agora tomar novas medidas para dar resposta às questões subjacentes imediatas e aproveitar as oportunidades proporcionadas pela IA no domínio da cibersegurança**.

O presente plano de ação constitui uma **resposta inicial e específica para ajudar os Estados-Membros e as organizações da União a enfrentarem esta nova realidade**.

Em primeiro lugar, a fim de garantir uma adoção segura e responsável, a UE reforçará a sua capacidade de avaliar a IA de fronteira antes do seu lançamento, nomeadamente no domínio da cibersegurança. Esse reforço promoverá um processo rigoroso de avaliação externa e capacidades de avaliação de alto nível na UE no domínio da IA. A UE facilitará igualmente o acesso dos intervenientes europeus a cibercapacidades avançadas baseadas na IA e apoiará os

[9] Regulamento (UE) 2025/38.
[10] JOIN(2025) 130 final.
[11] COM(2025) 148 final.
[12] Sifted, *Europe's most active deep tech investors in 2025*, 20 de março de 2026; relatório de impacto de 2025 do CEI.
[13] COM(2026) 502 final.

esforços para testar os modelos de IA disponíveis para utilizações no domínio da cibersegurança.

Em segundo lugar, a UE intensificará os esforços para apoiar os setores críticos e as pequenas e médias empresas (PME) na preparação para ciberameaças baseadas na IA, nomeadamente através da aplicação de princípios fundamentais em matéria de cibersegurança. Com base em toda a gama de IA disponível, a UE apoiará a sua utilização para reforçar a ciber-resiliência e corrigir as vulnerabilidades mais críticas.

Em terceiro lugar, a UE aumentará a sua capacidade para desenvolver e implantar soluções baseadas na IA, ao impulsionar um ecossistema europeu em torno destas e ao continuar a reforçar a sua própria capacidade de desenvolvimento de elementos de fronteira. A consecução deste último objetivo exigirá um investimento urgente e em grande escala em capitais próprios para reforçar as capacidades próprias da Europa em IA de fronteira, a fim de impulsionar soluções europeias que satisfaçam as nossas necessidades.

Por último, a UE trabalhará com parceiros que partilham das mesmas ideias em todos estes objetivos, a fim de promover uma abordagem mundial fiável e segura à IA de fronteira e à cibersegurança.

2. Pilar 1: garantir a segurança, a acessibilidade e a implantação da IA de fronteira para a cibersegurança europeia

Uma vez que as cibercapacidades avançadas baseadas na IA poderão, num futuro próximo, ser utilizadas como arma contra as nossas infraestruturas críticas e a nossa sociedade, a UE precisa, com caráter prioritário, de garantir uma sensibilização precoce para estas capacidades, de reforçar a capacidade técnica para avaliar os seus riscos, de criar oportunidades para testar o seu potencial de implantação no domínio da cibersegurança e de definir rotas de acesso mais claras para fins legítimos de cibersegurança na Europa. Para o efeito, e com base no quadro jurídico previsto no Regulamento IA, a UE alargará as capacidades europeias de avaliação antes dos lançamentos, estimulará uma abordagem europeia comum para aceder e coordenar os esforços de testagem, de modo que a IA de fronteira possa ser acedida e utilizada em segurança para efeitos de cibersegurança na Europa.

2.1. Avaliação e atenuação dos riscos colocados pela IA de fronteira

O Regulamento IA estabelece requisitos para a cibersegurança dos **sistemas de IA**[14] e **exige que os prestadores de modelos de IA de finalidade geral mais avançados avaliem e atenuem os riscos sistémicos**, nomeadamente decorrentes da utilização abusiva da IA no domínio do ciberespaço[15].

A partir de 2 de agosto de 2026, a Comissão exercerá os poderes de supervisão e execução previstos no Regulamento IA para assegurar uma supervisão eficaz dos sistemas de IA e dos modelos de IA de finalidade geral, incluindo modelos que apresentem riscos sistémicos

[14] Como parte do anexo III do Regulamento IA, os sistemas de IA utilizados em infraestruturas críticas serão considerados de risco elevado e estarão sujeitos a disposições específicas, nomeadamente em matéria de cibersegurança.

[15] No Regulamento IA, os riscos sistémicos são definidos como riscos específicos das capacidades de elevado impacto dos modelos de IA de finalidade geral que têm um impacto significativo no mercado da União devido ao seu alcance ou devido a efeitos negativos reais ou razoavelmente previsíveis na saúde pública, na segurança, na segurança pública, nos direitos fundamentais ou na sociedade no seu conjunto, que se pode propagar em escala ao longo da cadeia de valor (artigo 3.º, ponto 65, do Regulamento IA).

relacionados com a cibersegurança[16]. Esta supervisão inclui a avaliação da identificação feita pelos prestadores dos riscos associados às capacidades dos modelos, bem como das medidas que aplicaram para atenuar esses riscos. Estes requisitos continuam a ser proporcionais às capacidades da tecnologia em causa.

Os poderes de supervisão e execução serão apoiados pelo **painel científico que aconselha o Serviço para a IA da Comissão**, por **canais de comunicação seguros** e pelo **Código de Conduta sobre IA de Finalidade Geral**.

2.2. Construir a excelência europeia na avaliação da IA de fronteira antes do seu lançamento

A fim de promover a adoção segura e responsável da IA para a cibersegurança na UE, a ação regulamentar deve ser complementada por **capacidades de avaliação europeias reforçadas**. À medida que as capacidades de IA progridem e que os riscos sistémicos podem ocorrer não apenas no domínio do ciberespaço[17], a realização de avaliações externas surge como uma boa prática para garantir a segurança da IA de fronteira, em consonância com abordagens estabelecidas noutras indústrias que comportam riscos. O Regulamento IA salienta igualmente a **importância da avaliação antes da implantação** através de entidades terceiras, a fim de avaliar e atenuar os riscos sistémicos, conforme adequado. Até à data, a maioria das principais entidades que realizam avaliações de modelos de IA por terceiros antes da implantação está sediada fora da UE. Tendo em conta a sua importância crescente, torna-se urgente que alguns destes conhecimentos especializados em matéria de avaliação e as infraestruturas que lhes estão associadas se encontrem na UE.

Por conseguinte, a UE tem de reforçar os conhecimentos especializados disponíveis de modo a criar um ecossistema credível e competitivo de avaliadores terceiros para aferir as capacidades avançadas de IA e as medidas de atenuação dos riscos, apoiando a confiança no quadro de governação da IA da UE. Para o efeito, a Comissão proporá **critérios para avaliadores terceiros para efeitos do Código de Conduta sobre IA de Finalidade Geral e promoverá o desenvolvimento de um ecossistema de avaliação mais vasto.** Tal incluirá a facilitação de intercâmbios significativos entre avaliadores e peritos pertinentes, a fim de melhorar as metodologias de avaliação e clarificar os requisitos de qualificação.

No que diz respeito à **avaliação de modelos de IA especificamente para a cibersegurança**, a Europa tem potencial para liderar neste domínio com especialistas de alto nível em cibersegurança. Tendo em conta o contexto urgente, a UE deve potenciar e reforçar estes conhecimentos especializados. Para alcançar este objetivo, a Comissão lançará um convite específico à apresentação de propostas para a **criação de uma capacidade de avaliação da UE para modelos de IA que deve incluir a cibersegurança.** Esta capacidade dará um importante contributo para o ecossistema emergente na UE e basear-se-á no saber-fazer emergente em matéria de avaliação da IA nos Estados-Membros. Apoiará igualmente as

[16] Os poderes de execução relativos aos prestadores de modelos de IA de finalidade geral com risco sistémico que não cumpram as disposições relacionadas com a atenuação do risco sistémico abrangem a solicitação de informações sobre o modelo e de acesso ao modelo para realizar avaliações, medidas obrigatórias de atenuação dos riscos e, em última análise, a emissão de coimas até 3 % do volume de negócios anual a nível mundial ou a solicitação da restrição da disponibilização no mercado do modelo, da retirada ou recolha do mesmo por parte de um prestador.

[17] A título de exemplo, um outro domínio em que as capacidades dos modelos de IA de finalidade geral estão a aumentar continuamente e podem ser utilizadas de forma abusiva, com riscos para a saúde pública e para a segurança pública, é a biologia.

atividades regulamentares da Comissão realizadas através do Serviço para a IA[18], ao proporcionar uma escolha europeia para as avaliações por terceiros dos modelos de IA e respetivas medidas de atenuação. Contribuirá para a gestão dos riscos pelos prestadores, ao avaliar de forma independente as capacidades dos modelos e a eficácia das medidas de atenuação por parte dos prestadores de modelos[19].

Esta capacidade europeia apoiará os prestadores de modelos de IA de finalidade geral no cumprimento das obrigações pertinentes previstas no Regulamento IA, bem como os prestadores dos modelos do Código de Conduta sobre IA de Finalidade Geral[20]. Assegurará um processo de avaliação externa credível e rigoroso. As capacidades de avaliação de alto nível na UE contribuirão igualmente para a compreensão dos potenciais riscos sistémicos, nomeadamente no domínio da cibersegurança, mas também da biotecnologia e noutros domínios, ao produzirem sinais de alerta precoce quando os riscos são identificados.

2.3.Facilitar o acesso na UE a cibercapacidades avançadas baseadas na IA

O acesso a IA de fronteira com cibercapacidades avançadas rege-se cada vez mais por decisões específicas dos prestadores e, muitas vezes, não europeias, com alguns prestadores a limitar o acesso, para efeitos de gestão dos riscos de utilização abusiva, por meio de **programas de acesso estruturado** (por exemplo, lançamentos faseados de modelos). Embora essa restrição possa ser justificada por razões de segurança, esta prática carece frequentemente de transparência no que diz respeito aos critérios aplicados para determinar quais as organizações, incluindo as empresas, que obtêm acesso e através de que processo este é concedido. Esta situação pode prejudicar a capacidade de os intervenientes europeus, nomeadamente as autoridades competentes e os operadores de infraestruturas críticas, utilizarem atempadamente estas capacidades de IA e reforçarem a sua resiliência.

É urgentemente necessária uma abordagem coordenada a nível da UE, a fim de facilitar o acesso seguro e sem demora injustificada dos **intervenientes públicos e privados europeus** pertinentes a essa IA de fronteira. Para o efeito, a UE promoverá um processo avançado e baseado no risco, com critérios claros e concebido para atenuar eficazmente os riscos de utilização abusiva.

A Comissão, em coordenação com a Agência da União Europeia para a Cibersegurança (ENISA), elaborará um **plano de ação europeu para o acesso estruturado a capacidades avançadas de IA para fins de cibersegurança**, que servirá de documento de orientação para especificar a forma como os prestadores de IA com cibercapacidades avançadas podem conceder acesso a organizações europeias, incluindo empresas, apoiando assim a sua atenuação dos riscos de cibersegurança.

Este documento de orientação incluirá **os critérios que devem ser tidos em conta** para conceder aos intervenientes europeus acesso à IA com cibercapacidades avançadas. O plano

[18] O capítulo do Código de Conduta sobre IA de Finalidade Geral relativo à proteção e segurança exige que os prestadores realizem avaliações de modelos também através de avaliadores externos independentes devidamente qualificados (apêndice 3.5). Estes relatórios apoiarão então as atividades regulamentares do Serviço para a IA, uma vez que os prestadores são obrigados a apresentar a este serviço todos os relatórios disponíveis de avaliações externas juntamente com o modelo de relatório (medida 7.4).

[19] As avaliações realizadas no âmbito desta capacidade serão diferentes das realizadas na plataforma de testes prevista na secção 2.4. A plataforma será utilizada sobretudo para testar aplicações de cibersegurança de modelos de IA, ao passo que a capacidade se centrará na avaliação e atenuação do risco sistémico para apoiar o cumprimento do Código de Conduta.

[20] A capacidade não será um organismo de avaliação da conformidade, apenas apoiará a conformidade através das suas avaliações.

de ação deve abranger critérios pertinentes para diferentes tipos de organizações (por exemplo, instituições da UE, autoridades dos Estados-Membros, operadores de infraestruturas críticas, prestadores de serviços de cibersegurança e intervenientes no domínio da investigação) e descrever a forma como todos esses intervenientes serão identificados. Deve também incluir critérios de segurança para que o acesso concedido através do plano de ação não represente um risco indevido, bem como **um mecanismo para simplificar a concessão de acesso** às entidades elegíveis. Este mecanismo deve também facilitar a **informação** precoce por parte dos prestadores sobre os programas de acesso de confiança previstos, bem como a partilha de conhecimentos entre as organizações da UE às quais foi concedido acesso a um determinado modelo ou sistema.

Embora **não introduza novas obrigações para os prestadores**, o plano de ação apoiará os objetivos do Código de Conduta sobre IA de Finalidade Geral, ao identificar possíveis medidas de atenuação em matéria de segurança que possam complementar **a gestão dos riscos sistémicos** a aplicar pelos prestadores de modelos de IA de finalidade geral com risco sistémico[21][22]. Ao proporcionar um **quadro de referência europeu**, o plano de ação servirá de base para uma maior cooperação internacional.

O plano de ação deve incluir **medidas de contingência em caso de acesso restrito ou retirado a IA com cibercapacidades avançadas**, a fim de definir as ações a executar a nível da UE numa situação em que o acesso a um modelo ou sistema pertinente seja restringido ou retirado por um prestador ou por uma autoridade de um país terceiro. Além disso, quando for necessário um acesso atempado a IA de fronteira para utilização geral, a Comissão, em cooperação com os Estados-Membros, explorará a potencial utilização dos instrumentos de financiamento disponíveis, incluindo a contratação pública conjunta, para **obter conjuntamente acesso a esses modelos ou sistemas**.

2.4. Testar a IA com cibercapacidades avançadas para uma implantação atempada e segura da IA no domínio da cibersegurança

O acesso a uma IA de fronteira segura e fiável deve ser acompanhado de testes às suas capacidades de utilização em operações de cibersegurança, como a análise de vulnerabilidades, a reparação e a resposta a incidentes. Para colher os seus benefícios, os operadores de infraestruturas críticas e as autoridades públicas têm de compreender rapidamente o desempenho da IA com cibercapacidades avançadas em contextos realistas de cibersegurança, antes de ser implantada em ambientes sensíveis. Esses testes devem ser realizados em **ambientes seguros e controlados**.

Por conseguinte, a fim de criar sinergias a nível europeu, a **ENISA** e o **Centro Comum de Investigação da Comissão Europeia (JRC)**, em cooperação com outros serviços da Comissão e entidades da União competentes, como o Serviço de Cibersegurança para as Instituições, Órgãos e Organismos da União (CERT-UE), a Europol e as autoridades setoriais, bem como os Estados-Membros, organizarão uma **plataforma de testes segura para IA em utilizações no domínio da cibersegurança[23].** A plataforma permitirá que os participantes utilizem as suas próprias chaves de acesso aos modelos ao abrigo de regras de segurança e confidencialidade partilhadas, cobrindo cada um os seus próprios custos, utilizando as suas próprias ferramentas

[21] Em conformidade com o artigo 55.º, n.º 1, alínea b), do Regulamento IA.
[22] Por exemplo, o capítulo do Código de Conduta sobre IA de Finalidade Geral relativo à proteção e segurança refere, na medida 5.1, o «faseamento do acesso ao modelo» como um exemplo de atenuação em matéria de segurança.
[23] A plataforma existente gerida pelo JRC poderá ser melhorada para permitir este tipo de testes.

e mantendo a responsabilidade pelos seus métodos de teste. A ENISA, em coordenação com o JRC, deve regular o acesso à plataforma de testes e agregar os resultados.

Esta plataforma de testes segura da UE permitirá também **testar a implantação de cibercapacidades avançadas de IA em sistemas de infraestruturas críticas**, sem expor as infraestruturas reais a riscos («**centros virtuais de treinos**»[24]). Esta iniciativa dará prioridade à **adaptação e expansão dos centros virtuais de treinos existentes** e não à duplicação de ambientes. Em especial, embora sejam criados novos centros virtuais de treinos apenas em setores em que essas capacidades não estão atualmente disponíveis, todos os setores industriais poderão apoiar esta iniciativa, ao disponibilizar ambientes existentes a integrar através de compromissos específicos. Esses intervenientes da indústria podem receber informações agregadas das atividades de teste pertinentes, sob reserva das regras de confidencialidade aplicáveis.

A utilização deste ambiente centrar-se-á na testagem da IA para reforçar a ciber-resiliência e não visa avaliar a conformidade dos modelos de IA de finalidade geral com o Regulamento IA[25]. Promoverá e acelerará a experiência operacional com a utilização da IA para a ciber-resiliência, incluindo a deteção, a triagem, as informações sobre ameaças e a resposta, a fim de se antecipar aos ataques. A fim de assegurar um nível elevado de cibersegurança em toda a União, a **ENISA** basear-se-á nos seus conhecimentos para publicar e manter **orientações e conselhos sobre a utilização segura dos modelos e sistemas de IA disponíveis** para o ecossistema mais vasto.

Ações-chave:

- **Ação-chave 1 — A Comissão apoiará a criação de uma capacidade de avaliação da UE para modelos de IA que deve incluir a cibersegurança (2027).**
- **Ação-chave 2 — A Comissão, em coordenação com a ENISA, definirá um plano de ação europeu para o acesso estruturado a capacidades avançadas de IA para fins de cibersegurança, a fim de garantir que as organizações europeias possam aceder a essas capacidades de forma segura e atempada (T4 2026).**
- **Ação-chave 3 — A ENISA e o Centro Comum de Investigação da Comissão Europeia (JRC) criarão uma plataforma de testes segura para IA com cibercapacidades avançadas para utilizações no domínio da cibersegurança, a fim de impulsionar a implantação atempada e segura da IA na cibersegurança (T4 2026).**

3. Pilar 2: preparar o ecossistema de cibersegurança da UE para a era da IA

À medida que as cibercapacidades avançadas de IA se tornam cada vez mais acessíveis e amplamente implantadas, a UE deve estar preparada para fazer face à sua eventual utilização abusiva contra a sua economia e a sua sociedade e para as utilizar em segurança para efeitos de ciber-resiliência. A IA pode acelerar a descoberta de vulnerabilidades com um elevado grau de

[24] Os centros virtuais de treinos são ambientes seguros e controlados que reproduzem, de forma simulada, sistemas, redes ou infraestruturas digitais. Permitem testar em condições realistas, assegurando simultaneamente que qualquer atividade realizada no ambiente não afeta sistemas ou serviços reais.

[25] Testar a IA para efeitos de ciber-resiliência visa compreender a adequação operacional de um modelo de IA ou de um sistema de IA para executar uma tarefa específica de cibersegurança, ao passo que a avaliação dos modelos de IA para apoiar a conformidade com o Regulamento IA visa fornecer uma avaliação dos riscos decorrentes do modelo e da eficácia das medidas de atenuação dos riscos aplicadas pelo prestador do modelo. Testar a IA para efeitos de ciber-resiliência é, por conseguinte, diferente de avaliar modelos de IA para apoiar a conformidade com o Regulamento IA e exige competências e recursos diferentes.

automatização e em maior escala, reduzindo simultaneamente os conhecimentos especializados, o tempo e os recursos necessários para que intervenientes mal-intencionados realizem ataques sofisticados. Como prioridade imediata, a UE deve reforçar a sua preparação e apoiar setores críticos na adaptação a estas ameaças, o que inclui a integração de soluções de IA disponíveis nas operações de cibersegurança, tirando partido de toda a gama de modelos de IA e, em especial, dos que são de fonte aberta, agilizando simultaneamente os esforços para identificar e corrigir as vulnerabilidades mais críticas. A ENISA está numa posição privilegiada para apoiar esta transição do ecossistema de cibersegurança da UE para a era da IA.

3.1. Aplicação dos princípios fundamentais e da preparação da UE em matéria de cibersegurança

Neste novo panorama tecnológico e de segurança, **os princípios fundamentais e a preparação em matéria de cibersegurança são agora mais importantes do que nunca**, devendo as ferramentas e os instrumentos de cibersegurança existentes na UE ser plenamente utilizados.

O quadro regulamentar da UE em matéria de cibersegurança, nomeadamente **a Diretiva SRI 2[26] e o Regulamento Resiliência Operacional Digital**, proporciona uma base de referência sólida para a preparação das infraestruturas críticas contra todos os tipos de riscos de cibersegurança, incluindo os relacionados com a IA. Por conseguinte, estas regras devem ser transpostas e aplicadas pelos Estados-Membros com caráter de urgência. Além disso, os Estados-Membros devem ter em conta os riscos decorrentes da IA avançada no seu trabalho de supervisão. Do mesmo modo, os operadores de setores críticos e as entidades financeiras devem analisar e ajustar o seu quadro de gestão dos riscos às novas realidades, antecipando ciberataques baseados na IA mais frequentes e em maior escala, bem como reduzir o tempo necessário para a correção, acelerando a cadência das correções e tendo a capacidade de corrigir rapidamente sistemas complexos.

A fim de reforçar ainda mais a preparação, as entidades devem aplicar de forma coerente **medidas básicas de ciber-higiene** e introduzir uma solidez das redes e dos sistemas (nomeadamente através de abordagens de «confiança zero», se for caso disso). Devem também começar a **utilizar as capacidades de IA já disponíveis**, nomeadamente por meio de modelos de fonte aberta, para detetar vulnerabilidades e melhorar a deteção e prevenção de ciberataques. As **entidades da União**, com o apoio do CERT-UE e com as orientações do Conselho Interinstitucional para a Cibersegurança, podem dar o exemplo a este respeito para reforçar a postura global da União no ciberespaço, em conformidade com o regulamento relativo à cibersegurança das entidades da União[27]. Os Estados-Membros são também fortemente incentivados a utilizar plenamente as possibilidades de conversão da **Reserva de Cibersegurança da UE** para reforçar a resiliência contra ciberameaças baseadas na IA, nomeadamente através da análise da vulnerabilidade, de testes de penetração automatizados e da monitorização dos riscos, com apoio para recomendações de correção.

Além disso, tal como refletido no **Regulamento de Ciber-Resiliência**, que será plenamente aplicável a partir de 11 de dezembro de 2027, continua a ser essencial o desenvolvimento seguro desde a conceção, a gestão sistemática das vulnerabilidades, a correção atempada e práticas de codificação segura, incluindo abordagens que eliminem classes inteiras de

[26] A Diretiva SRI 2 estabelece a base de referência para a gestão dos riscos de cibersegurança, exigindo que as entidades essenciais e as entidades importantes que operam em 18 setores críticos protejam as suas redes e sistemas de informação e previnam e minimizem o impacto dos incidentes.
[27] Regulamento (UE, Euratom) 2023/2841.

vulnerabilidades, como o desenvolvimento de *software* de memória segura. Os riscos de cibersegurança específicos da IA, nomeadamente a contaminação de dados e de modelos, ataques antagónicos e a injeção de instruções, devem também ser cuidadosamente avaliados e atenuados, em conformidade com as disposições pertinentes do Regulamento IA.

Para apoiar estes esforços, a **ENISA**, em cooperação com as autoridades europeias de supervisão e outras entidades competentes da União, irá disponibilizar e gerir **orientações, recomendações, conselhos e boas práticas para assegurar uma proteção contínua contra ameaças baseadas na IA[28] e promover a integração segura de ferramentas de IA em operações de cibersegurança**. Essas orientações e conselhos devem também ter em conta as necessidades das PME mais vulneráveis a ataques. Se for caso disso, é possível envidar e reforçar estes esforços através de iniciativas setoriais e mecanismos de cooperação em domínios como as finanças, os transportes, a energia, o setor agroalimentar, os cuidados de saúde[29] e o espaço.

À medida que as tecnologias e os riscos associados continuarem a evoluir, **o conhecimento coletivo da situação e a partilha estruturada de informações sobre ameaças à cibersegurança baseadas na IA** através das redes pertinentes da União, tanto a nível horizontal como setorial, serão fundamentais para reforçar o conhecimento da situação. A ENISA deve explorar formas de apoiar a cooperação com os prestadores de IA, a fim de reforçar a partilha de informações sobre ameaças.

Do mesmo modo, os Estados-Membros devem tirar partido das estruturas existentes a nível da União no domínio da cibersegurança para **avaliar a preparação das infraestruturas críticas**, trabalhando em conjunto, em especial no âmbito do grupo de cooperação Segurança das Redes e da Informação (SRI) e, se for caso disso, em cooperação com o Comité para a Inteligência Artificial criado ao abrigo do Regulamento IA.

3.2. Acelerar o processo de correção: melhorar a gestão das vulnerabilidades para a descoberta à velocidade da IA

O desafio imediato para a postura da UE no ciberespaço consiste em **corrigir as vulnerabilidades existentes antes que possam ser exploradas em grande escala**. Uma vez que a IA reduz o tempo necessário para que os intervenientes mal-intencionados explorem vulnerabilidades, as entidades competentes devem igualmente acelerar a sua capacidade de analisar, priorizar, corrigir e implantar soluções com rapidez suficiente para prevenir a exploração.

Os processos de tratamento de vulnerabilidades existentes devem ser melhorados, para que sejam eficazes na era da descoberta apoiada pela IA. A ENISA deve assegurar que as infraestruturas e os serviços europeus de gestão das vulnerabilidades, incluindo a base de dados de vulnerabilidades da União Europeia e a plataforma única de comunicação de informações do Regulamento de Ciber-Resiliência, são adequados à sua finalidade na era da descoberta de vulnerabilidades apoiada pela IA e, em conjunto com os Estados-Membros, reforçam a interoperabilidade entre as plataformas e bases de dados de vulnerabilidades da UE, nacionais e mundiais.

---

[28] Um exemplo dessas recomendações é a publicação no blogue do CERT-UE: *AI is changing the economics of vulnerability discovery. Defenders should adapt now,* 21 de abril de 2026.

[29] Plano de Ação Europeu para a Cibersegurança dos Hospitais e dos Prestadores de Cuidados de Saúde: COM(2025) 10 final.

Com o aumento do número de relatórios de vulnerabilidades, os fabricantes têm de decidir quais as falhas a corrigir em primeiro lugar em todas as linhas de produtos, ao passo que os utilizadores, especialmente as entidades essenciais e de importância crítica, têm de determinar quais as atualizações a implantar em primeiro lugar, muitas vezes com recursos limitados. As organizações devem poder contar com orientações claras a nível da UE, baseadas no risco e alinhadas com o Regulamento de Ciber-Resiliência e a Diretiva SRI 2, a fim de ajudar a corrigir os casos em que os riscos são maiores.

No âmbito das suas obrigações ao abrigo da Diretiva SRI 2, **os Estados-Membros devem também atualizar as políticas nacionais de divulgação coordenada de vulnerabilidades** para fazer face à exploração baseada na IA. O grupo de cooperação SRI deve rever as suas orientações sobre a divulgação coordenada de vulnerabilidades e a UE deve também analisar se as normas ISO/IEC subjacentes aos quadros em matéria de divulgação coordenada de vulnerabilidades continuam a ser adequadas à sua finalidade à luz das ameaças atuais. A cooperação internacional é igualmente essencial a este respeito, uma vez que estas práticas são moldadas a nível mundial.

Por último, a segurança das infraestruturas críticas não se limita à divulgação de vulnerabilidades ou ao lançamento de soluções. O maior desafio reside na **sua aplicação**. À medida que a IA acelera a descoberta de vulnerabilidades, o estrangulamento na aplicação de correções torna-se mais acentuado. Com o apoio da ENISA, os Estados-Membros devem tirar partido das redes existentes, como o grupo de cooperação SRI, para fazer face a este desafio, que é da maior urgência.

3.3. Pôr em prática: corrigir o que é mais importante

A UE não deve apenas desenvolver conhecimentos sobre a forma como a IA pode reforçar a ciber-resiliência; deve **aplicar esses conhecimentos nos casos em que a necessidade é mais urgente**. Por conseguinte, o desafio consiste não só em encontrar vulnerabilidades mais rapidamente, mas também em analisá-las, corrigi-las e coordenar a implantação em grande escala. **O *software* crítico de fonte aberta é o domínio em que se devem tomar medidas prioritárias**, devido à elevada penetração em setores de infraestruturas críticas. Alegadamente, 98 % da base de códigos total contém fonte aberta, com a indústria das infraestruturas críticas a representar, em média, cerca de 80 % das bases de códigos com vulnerabilidade de risco elevado ou crítico[30].

A **Estratégia da UE para a Fonte Aberta**[31], publicada no âmbito do pacote de soberania tecnológica, inclui uma série de medidas para aumentar a segurança e apoiar a manutenção de componentes críticos de fonte aberta. Neste contexto, a Comissão trabalhará com a ENISA, os Estados-Membros[32] e as comunidades de fonte aberta para testar algumas ações especificamente orientadas para o ciberespaço e a IA.

A ENISA, em cooperação com a Comissão, os Estados-Membros e as comunidades de fonte aberta, acelerará o levantamento dos componentes críticos de fonte aberta previstos na estratégia e, com base numa lista preliminar baseada em critérios acordados, **testará uma campanha de resiliência crítica de fonte aberta** para componentes de fonte aberta relevantes para as infraestruturas críticas. Os resultados da campanha contribuirão para a aplicação do

[30] Blackduck, *Open Source Security and Risk Analysis Report*, 2026: por exemplo, para os setores aeroespacial, da aviação, automóvel, dos transportes e da logística — 87 %; indústrias transformadoras — 88 %; cuidados de saúde — 88 %; energia — 89 %; infraestruturas de Internet e de *software* — 80 %.
[31] COM(2026) 503 final.
[32] Em especial, se for caso disso, em coordenação com o Consórcio para uma Infraestrutura Digital Europeia para os Bens Comuns Digitais.

instrumento de manutenção de fontes abertas. A campanha consistirá num regime de patrocínio voluntário para fazer corresponder projetos de fonte aberta a organizações dispostas a trabalhar em parceria estreita com os responsáveis pela manutenção dos projetos, a fim de apoiar a sua manutenção e segurança. Os patrocinadores podem incluir Estados-Membros, entidades da União como o CERT-UE, operadores de infraestruturas críticas, fabricantes e outras entidades públicas ou privadas capazes de prestar apoio, por exemplo, disponibilizando pessoas qualificadas ou modelos e ferramentas de IA aos responsáveis pela manutenção de projetos de fonte aberta. Os Estados-Membros e outros utilizadores elegíveis podem recorrer ao apoio de prestadores privados de confiança constantes da **Reserva de Cibersegurança da UE** para uma análise da vulnerabilidade das dependências de fonte aberta em infraestruturas críticas. Além disso, a ENISA criará um **catálogo de serviços alimentados por IA**, destinado a apoiar a correção e a reparação de vulnerabilidades de fonte aberta.

Os responsáveis pela manutenção de fonte aberta poderão beneficiar do regime de patrocínio e do catálogo de serviços para aumentar a rapidez e a eficácia do seu trabalho e reduzir os riscos de cibersegurança, intensificados pela evolução dos modelos de IA. A iniciativa reforçará a governação e os fluxos de trabalho de fonte aberta existentes e servirá de base para a pressão mais ampla da Europa no sentido da reparação assistida por IA, reforçando ainda mais o saber-fazer operacional da União. Contribuirá para reforçar a ciber-resiliência em todos os setores, incluindo as infraestruturas críticas e as PME. Em 2026, será lançada uma primeira campanha-piloto com vista a uma maior expansão, se esta se revelar bem-sucedida, nomeadamente no contexto da Estratégia para a Fonte Aberta.

Ações-chave

- **Ação-chave 4 — A ENISA, em cooperação com as entidades competentes da União, emitirá orientações, recomendações, conselhos e boas práticas sobre a proteção contra ameaças baseadas na IA e para a integração segura da IA em operações de cibersegurança (a partir do T3 2026)**
- **Ação-chave 5 — A Comissão, os Estados-Membros, a ENISA e a indústria cooperarão com vista a adaptar as atuais práticas e ferramentas de gestão das vulnerabilidades à era da IA (a partir do T3 2026)**
- **Ação-chave 6 — A ENISA, em cooperação com a Comissão, os Estados-Membros, as comunidades de fonte aberta, as entidades da União e a indústria, lançará um primeiro projeto-piloto de uma campanha de resiliência crítica de fonte aberta para acelerar as correções, nomeadamente através da mobilização da IA (T4 2026)**

4. Pilar 3: expandir as capacidades europeias de IA para o ciberespaço

Num contexto em que as ciberoperações, quer defensivas, quer ofensivas, dependem cada vez mais da IA avançada, a capacidade de desenvolver e implantar soluções de cibersegurança baseadas na IA está a tornar-se um facilitador estratégico da ciber-resiliência e da soberania. Em especial, nos casos de utilização considerados sensíveis, a UE deve poder contar com capacidades soberanas de IA que satisfaçam as necessidades de segurança, nomeadamente no domínio da defesa. A UE deve agora permitir que os prestadores europeus, incluindo os inovadores disruptivos, desenvolvam, implantem e expandam essa IA avançada na Europa. Complementando a sua estratégia de investimento no domínio do ciberespaço e da IA, a UE deve reunir o seu ecossistema tecnológico para dar resposta às necessidades operacionais mais urgentes em matéria de cibersegurança, promover investimentos no desenvolvimento e na

adoção de capacidades europeias de IA rumo à fronteira e desenvolver as competências necessárias para as implantar em todos os setores.

4.1. Impulsionar o ecossistema europeu em torno de soluções de cibersegurança baseadas na IA

Uma vez que a IA já é aproveitada para fins maliciosos, as organizações têm de avançar mais rapidamente do que os atacantes na implantação de soluções de cibersegurança baseadas na IA disponíveis para proteger as infraestruturas críticas em todos os setores. A UE deve encorajar o mercado europeu a disponibilizar esses instrumentos à velocidade e à escala necessárias e incentivar a adoção nas nossas infraestruturas críticas.

A UE já está a realizar investimentos significativos para **apoiar a investigação e o desenvolvimento de tecnologias internas avançadas de cibersegurança baseadas na IA** e a favor da cibersegurança da IA, nomeadamente com 200 milhões de EUR até ao final do atual quadro financeiro plurianual no âmbito dos programas Horizonte Europa e Europa Digital. Por exemplo, no final de 2026, serão lançados três projetos emblemáticos do Horizonte Europa para apoiar o desenvolvimento, a formação e a testagem de IA para capacidades de monitorização, deteção, resposta e autorreparação em processos e sistemas digitais contra ciberataques, incluindo ataques antagónicos de IA, bem como o desenvolvimento de ferramentas e tecnologias de IA generativa para a monitorização contínua, a conformidade e a reparação automatizada. A UE está também a financiar todo o ciclo de capacidades de IA no que diz respeito à aplicação da lei, desde a investigação até à testagem, validação e implantação operacional através do Horizonte Europa, do Fundo para a Segurança Interna, do Europa Digital e da Comunidade Europeia de Investigação e Inovação para a Segurança. Do mesmo modo, a UE investe, através do Conselho Europeu da Inovação (CEI), nomeadamente por meio de investimentos diretos do Fundo do CEI, em empresas europeias de cibersegurança e IA de tecnologia profunda, estendendo-se também, em 2026 e 2027, às tecnologias de defesa estratégicas e de dupla utilização pertinentes[33]. Mais especificamente, até ao final de 2026, a Comissão permitirá que os investimentos do Fundo do CEI em empresas de cibertecnologia e de tecnologia de IA, no montante de 100 milhões de EUR, sejam investidos em empresas tecnológicas estratégicas em fase de arranque e em fase de expansão no domínio da defesa e prossigam um apoio semelhante em 2027. O Fundo Europeu para Empresas em Fase de Expansão fará o seu primeiro investimento na etapa de crescimento de empresas estratégicas ainda em 2026. Com base na Estratégia Digital Internacional para a UE, a UE e os Estados-Membros tirarão também partido da oferta de empresas tecnológicas da UE para apoiar a implantação de soluções de IA e de *software*.

Em complemento destes investimentos, a União deve procurar **acelerar ainda mais a partilha de conhecimentos sobre capacidades avançadas de cibersegurança baseadas na IA contra ciberataques em grande escala que utilizem a IA**. Atualmente, a UE dispõe de um ecossistema rico e de uma base de conhecimentos em todo o meio académico, na indústria e na administração pública, mas as soluções baseadas na IA para a cibersegurança continuam fragmentadas, insuficientemente testadas em ambientes operacionais e longe de serem implantadas em grande escala em todos os setores[34]. Um exemplo é a reparação automatizada de vulnerabilidades, que é um dos principais estrangulamentos operacionais da cibersegurança na era da IA: atualmente, a descoberta de vulnerabilidades baseada na IA está a avançar mais rapidamente do que a reparação assistida pela IA, criando assim um desequilíbrio estrutural em benefício dos atacantes. Por conseguinte, em resposta aos apelos para fazer face às ameaças

[33] Fundo do CEI — Conselho Europeu da Inovação — Comissão Europeia.
[34] *Public Letter of Support for a European Grand Challenge in AI and Security* — Google Docs.

colocadas pela IA ofensiva[35], a Comissão, com o apoio do Centro Europeu de Competências em Cibersegurança (ECCC) e em cooperação com a ENISA, lançará um **Grande Desafio da UE dedicado à reparação de vulnerabilidades assistida pela IA**. Reunindo empresas europeias de cibersegurança e de IA, organizações de investigação, operadores de infraestruturas críticas e comunidades de fonte aberta em torno desta missão comum, o grande desafio apoiará o desenvolvimento de um sistema de IA capaz de prestar assistência a equipas de cibersegurança ao longo do ciclo de vida da reparação. Ao ligar a investigação e a implantação, o grande desafio permitirá testar soluções promissoras em ambientes operacionais realistas e, em última análise, disponibilizá-las a organizações em toda a Europa, contribuindo para reduzir os estrangulamentos operacionais que dificultam a reparação atempada. Os Estados-Membros interessados serão convidados a apoiar esses esforços de partilha de conhecimentos.

4.2. Criar capacidades de fronteira europeias

Embora os modelos e sistemas de IA existentes com capacidades de cibersegurança já proporcionem oportunidades significativas para operações nesse âmbito, as cibercapacidades de fronteira baseadas na IA têm também implicações importantes para a soberania tecnológica, a segurança e a defesa da Europa. Por conseguinte, a UE deve **desenvolver as suas próprias capacidades soberanas de IA de fronteira de finalidade geral** para atenuar o risco de novas dependências em relação ao que se tornou agora um ativo estratégico crítico, com um potencial de dupla utilização cada vez maior da IA de fronteira que se estende muito para além do domínio da cibersegurança. Constitui um desafio transetorial mais vasto para a nossa economia e para a nossa sociedade, que a Comissão continuará a acompanhar de perto e a enfrentar à medida que evolui.

A Comissão já tomou medidas concretas para apoiar os principais intervenientes europeus na promoção das capacidades de IA rumo à fronteira.

- Recentemente, a Comissão atribuiu o Grande Desafio da IA de Fronteira (*Frontier AI Grand Challenge*), concedendo acesso à capacidade de computação da Empresa Comum HPC e apoiando o desenvolvimento de um modelo europeu de IA avançada de fonte aberta[36].
- No âmbito do Recurso para a Ciência da IA na Europa (RAISE), a Comissão está a financiar uma rede de laboratórios de IA de fronteira para fazer avançar a investigação também neste domínio.
- No âmbito do Horizonte Europa, a Comissão está a financiar atividades destinadas a expandir a IA segura e protegida rumo à fronteira.
- A Comissão continuará a trabalhar com a França e a Alemanha para criar um esforço de colaboração (a «Iniciativa Europeia IA de Fronteira»), prosseguindo as apostas em investigação e inovação, atraindo talentos e facilitando as empresas derivadas.
- A Comissão beneficia de aconselhamento técnico através do fórum sobre IA de fronteira[37].

Estas medidas iniciais constituem uma base importante, mas **é necessária uma mudança de paradigma em termos de ambição e recursos** para transformar as aspirações da Europa em matéria de IA de fronteira numa capacidade soberana duradoura e numa vantagem competitiva.

---

[35] *Idem*.

[36] Comissão seleciona o consórcio EUROPA como vencedor do Grande Desafio da IA de Fronteira, um projeto para construir um modelo europeu de IA de fronteira de fonte aberta nas 24 línguas da UE — Construir o futuro digital da Europa.

[37] Comissão procura peritos para fórum sobre IA de fronteira |Construir o futuro digital da Europa.

Dada a escala sem precedentes dos recursos necessários para o desenvolvimento da IA de fronteira, os projetos de fronteira exigem uma abordagem colaborativa a nível da União. O ato legislativo sobre o desenvolvimento da nuvem e da IA proposto identifica-os como projetos prioritários e atribui recursos de computação da União que complementam os atribuídos pelos Estados-Membros. **As fábricas de IA existentes e as futuras gigafábricas** devem ser aproveitadas para funcionar como parte de uma infraestrutura europeia soberana para a IA e a cibersegurança, incluindo computação, dados e conectividade, e para posicionar a UE como um continente líder no domínio da IA. Essa conectividade é um requisito prévio para a partilha fiável de conjuntos de dados preparados para a IA, para a federação de recursos além-fronteiras, para o funcionamento seguro de ambientes controlados e para o desenvolvimento, testagem, implantação e acesso a cibercapacidades sólidas, fiáveis e de elevado desempenho baseadas em IA. As fábricas de IA pertinentes centradas no ciberespaço devem facilitar o acesso a conjuntos de dados de elevada qualidade preparados para a IA, desde dados públicos a dados industriais[38] e de cibersegurança sensíveis, através de mecanismos de partilha de dados fiáveis, seguros e resilientes, bem como apoiar o desenvolvimento e a validação de modelos de IA num ambiente controlado, responsável e auditável através dos seus laboratórios de dados.

A Comissão apoiará igualmente o desenvolvimento de cibercapacidades europeias soberanas no domínio da IA, nomeadamente para a defesa, através do Fundo Europeu de Competitividade (FEC), assegurando que a Europa está mais bem equipada para proteger os seus interesses estratégicos e reduzir as dependências críticas. Neste contexto, a Comissão criará um grupo de trabalho específico com as agências competentes, incluindo a ENISA e a Agência Europeia de Defesa (AED), e os Estados-Membros para fazer face aos riscos de segurança associados à implantação de modelos de IA de fronteira em sistemas críticos de defesa e de dupla utilização.

O desenvolvimento de capacidades de fronteira soberanas implicará **centenas de milhares de milhões de EUR de necessidades de investimento** que só podem ser parcialmente cobertas pelas finanças públicas, o que exige a mobilização urgente de grandes montantes de investimento privado e, em especial, de capital de risco e de capitais próprios para desenvolver e expandir soluções europeias inovadoras. Sem computação, modelos e infraestruturas de dados, a Europa continuará a ser um utilizador vulnerável de sistemas de IA de fronteira fabricados noutros locais, que outros podem desligar subitamente — com enormes implicações económicas e de (ciber)segurança. No entanto, embora o custo para a Europa de construir a sua própria capacidade de IA de fronteira possa ser muito elevado, o custo de não a construir pode ser ainda maior e aumentar todos os anos à medida que o défice de capacidade de IA aumenta.

Com o seu pacote de soberania tecnológica, de 3 de junho de 2026, a Comissão lançou **consultas com os Estados-Membros, o Grupo BEI e outras partes interessadas fundamentais sobre a proposta de criação de uma nova capacidade europeia de capitais próprios** para gerir uma carteira de investimentos em capitais próprios em grande escala em tecnologias avançadas e infraestruturas essenciais para a nossa soberania tecnológica — incluindo tecnologias digitais como a IA de fronteira, mas também tecnologias de energia limpa, biotecnologia e, potencialmente, tecnologias de defesa. A principal vantagem deste mecanismo será a criação de uma «âncora de coinvestimento» de capitais próprios extremamente necessária que atrairá grandes quantidades de investimentos privados, trabalhando em sinergia com instrumentos financeiros já existentes a nível da UE, como o Fundo Europeu para Empresas em Fase de Expansão, ou investindo nesses instrumentos financeiros. Este novo mecanismo estratégico de capitais próprios para a tecnologia será um fator de mudança na resposta a este último apelo à realização de grandes investimentos da UE

[38] Sob reserva do cumprimento da legislação aplicável, incluindo o direito da concorrência da UE.

em IA de fronteira. No que diz respeito ao Instrumento InvestEU do FEC, esse mecanismo poderá tornar-se um interveniente importante no domínio dos investimentos estratégicos em capitais próprios de grandes montantes em tecnologias e infraestruturas avançadas.

4.3.Reforçar as competências em matéria de cibersegurança para a era da IA

A tecnologia, por si só, não determinará o êxito da Europa. A capacidade de implantar uma IA avançada de forma eficaz e segura em operações de cibersegurança dependerá também da **disponibilidade de profissionais qualificados capazes de compreender e utilizar em segurança modelos de IA com cibercapacidades avançadas**, bem como de gerir riscos específicos da IA. Uma vez que as equipas de cibersegurança integrarão cada vez mais a IA avançada, esta situação poderá agravar ainda mais o atual défice de competências em matéria de cibersegurança. Por conseguinte, a UE deve reforçar a sua mão de obra no domínio da cibersegurança, dotando-a das competências adequadas em matéria de IA para a cibersegurança.

A **Academia de Competências de Cibersegurança da UE**, que reúne a indústria, os prestadores de formação e as instituições académicas em torno de compromissos e parcerias concretos em matéria de formação em cibersegurança, proporciona o quadro adequado para dar resposta a esta necessidade a nível da União. A Comissão, juntamente com os Estados-Membros, mobilizará este ecossistema crescente para lançar uma ação específica no âmbito da Academia de Cibercompetências, a fim de criar programas de formação para que os profissionais da cibersegurança utilizem ferramentas de IA. Deve também explorar potenciais sinergias com a futura Academia de Competências em IA. Além disso, a ENISA atualizará o **Quadro Europeu de Competências em Cibersegurança**, integrando competências relacionadas com a IA nos perfis profissionais existentes e definindo novas funções sempre que necessário.

Ações-chave:

- **Ação-chave 7 — A Comissão, com o apoio do Centro Europeu de Competências em Cibersegurança e em cooperação com a ENISA, lançará um grande desafio da UE para ajudar a expandir as soluções europeias de cibersegurança baseadas na IA (T4 2026)**
- **Ação-chave 8 — A Comissão, juntamente com os Estados-Membros, procurará disponibilizar o acesso à capacidade de computação das fábricas de IA para testar, treinar e implantar modelos de IA avançados e de fronteira disponíveis para a ciber-resiliência em computação soberana.**
- **Ação-chave 9 — A Comissão colaborará com os Estados-Membros e a indústria (no âmbito da Academia de Competências de Cibersegurança) para desenvolver módulos de formação para os profissionais da cibersegurança sobre a utilização da IA para a cibersegurança (T4 2026).**

5. Trabalhar com parceiros que partilham as mesmas ideias no sentido de uma abordagem mundial da cibersegurança na era da IA

As implicações da IA para a cibersegurança são intrinsecamente mundiais, uma vez que os modelos e sistemas de IA, as cadeias de abastecimento de *software* e os ecossistemas de fonte aberta funcionam além-fronteiras. O lançamento de um modelo de IA com cibercapacidades desenvolvido numa jurisdição pode ter consequências significativas para a segurança das

infraestruturas críticas e das empresas em todo o mundo. Os governos, as organizações internacionais e a indústria enfrentam, assim, **um desafio comum, sendo a cooperação internacional essencial** para evitar a fragmentação, promover a interoperabilidade entre parceiros de confiança e congregar esforços para atenuar os riscos de cibersegurança associados à IA.

A UE deve liderar a definição de práticas mundiais em matéria de IA de confiança e de ciber-resiliência, tirando partido do **quadro regulamentar da União em matéria de IA e de cibersegurança**. Em especial, é necessária uma cooperação mais estreita entre parceiros que partilham as mesmas ideias para garantir que as capacidades de IA de fronteira permanecem seguras e disponíveis para utilizações de confiança, evitando simultaneamente a sua utilização abusiva por intervenientes mal-intencionados. O presente plano de ação constitui também um apelo aos nossos parceiros internacionais para que se associem aos esforços para amplificar o impacto das medidas propostas em matéria de segurança da IA e ciber-resiliência.

Em especial, a Comissão prosseguirá estes objetivos em instâncias bilaterais e multilaterais. Continuará a participar ativamente no **G7 para promover a sua abordagem**, nomeadamente através dos **grupos de trabalho sobre tecnologias digitais e cibersegurança**, a fim de apoiar os trabalhos no sentido de um entendimento comum dos riscos de cibersegurança decorrentes de capacidades avançadas de IA. A Comissão promoverá a cooperação do G7 em matéria de normas e avaliação destes modelos. Convida igualmente os membros do G7 e outros parceiros internacionais a unirem esforços para apoiar a segurança do *software* de fonte aberta e a cooperarem na adaptação de práticas de gestão da vulnerabilidade. A UE continuará também a participar nos trabalhos das Nações Unidas.

A nível bilateral, a UE aprofundará os intercâmbios com países parceiros em matéria de IA avançada e cibersegurança, nomeadamente através de parcerias digitais, diálogos digitais ou ciberdiálogos, e dará prioridade à avaliação dos modelos, à proteção das infraestruturas críticas, à atenuação das vulnerabilidades e à melhoria da ciber-resiliência como domínios fundamentais de cooperação, conforme adequado.

Além disso, a **Rede de Medição, Avaliação e Ciência da IA Avançada (*Network of Advanced AI Measurement, Evaluation and Science*), coordenada pelo Instituto de Segurança de IA do Reino Unido (AISI)** e em estreita colaboração com os institutos de segurança e proteção de países parceiros e o **Serviço para a IA da Comissão**, é uma plataforma importante para o desenvolvimento de metodologias comuns para a avaliação de modelos de IA de fronteira, o intercâmbio de boas práticas e o apoio a uma cooperação internacional de confiança em matéria de segurança e proteção da IA.

A Comissão incentivará igualmente um diálogo estruturado entre os governos e os principais criadores de IA de fronteira, a fim de promover abordagens comuns em matéria de segurança, avaliação e implantação responsável da IA de fronteira.

Por último, tendo em conta as referidas implicações para a segurança europeia e nacional, a UE reforçará os intercâmbios existentes com a **OTAN** sobre as oportunidades e os riscos associados às capacidades de IA de fronteira no domínio do ciberespaço, nomeadamente tirando partido do futuro Centro de Excelência da OTAN para a Inteligência Artificial.

6. Conclusão

O presente plano de ação marca a continuação de um esforço europeu sustentado e coordenado. Uma vez que o desenvolvimento de capacidades avançadas de IA continuará a acelerar, com o surgimento de novas oportunidades e riscos, a Comissão avaliará regularmente a execução do plano de ação e adaptará as ações sempre que necessário, a fim de assegurar que contribui

eficazmente para o desenvolvimento de um ecossistema europeu seguro e resiliente para a era da IA.