C/2026/3795

16.7.2026

ALERTA DO COMITÉ EUROPEU DO RISCO SISTÉMICO

de 25 de junho de 2026

sobre os ciber-riscos sistémicos decorrentes de modelos de inteligência artificial de fronteira

(CERS/2026/3)

(C/2026/3795)

O CONSELHO GERAL DO COMITÉ EUROPEU DO RISCO SISTÉMICO,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Acordo sobre o Espaço Económico Europeu ([1]), nomeadamente o anexo IX,

Tendo em conta o Regulamento (UE) n.º 1092/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, relativo à supervisão macroprudencial do sistema financeiro na União Europeia e que cria o Comité Europeu do Risco Sistémico ([2]), nomeadamente o artigo 3.º, n.º 2, alínea c) e os artigos 16.º e 18.º,

Tendo em conta a Decisão CERS/2011/1 do Comité Europeu do Risco Sistémico, de 20 de janeiro de 2011, que adota o Regulamento Interno do Comité Europeu do Risco Sistémico ([3]), nomeadamente os artigos 18.º e 19.º,

Considerando o seguinte:

(1) Os principais fornecedores de inteligência artificial (IA) desenvolveram Modelos de IA de Fronteira (*Frontier AI Models* — FAIM), que são altamente capazes no domínio da cibersegurança e capazes de realizar ciberataques totalmente automatizados a sistemas complexos, nomeadamente através da descoberta de vulnerabilidades e do desenvolvimento e da conversão em arma de explorações de vulnerabilidades, alterando assim fundamentalmente o panorama das ciberameaças.

(2) Os FAIM são significativamente melhores do que os modelos de IA anteriores na procura de formas de realizar ciberataques, superando os modelos anteriores em termos de custos, velocidade e exatidão, rivalizando agora com os principais peritos humanos.

(3) Os FAIM têm a capacidade de ameaçar os sistemas subjacentes aos ambientes das tecnologias da informação e comunicação (TIC) em que assenta a infraestrutura financeira, aumentando a probabilidade e a gravidade de ciberincidentes com impacto sistémico.

(4) Os FAIM demonstraram a sua capacidade para descobrir vulnerabilidades e desenvolver novas técnicas de exploração de vulnerabilidades, expondo assim os principais sistemas operativos e software utilizados em quase todos os ambientes TIC das organizações ao risco de ciberataques.

(5) Historicamente, a descoberta de tais vulnerabilidades tem sido rara e frequentemente efetuada por investigadores no domínio da segurança, permitindo uma correção direcionada. Nesses casos, os fornecedores de software dispõem frequentemente de um prazo normalizado — geralmente de 90 dias — para corrigir a vulnerabilidade antes da sua divulgação pública. No entanto, é provável que os FAIM aumentem o volume de vulnerabilidades detetadas.

(6) As atuais práticas de correção (*patching*) no sistema financeiro são predominantemente reativas, baseando-se em atualizações periódicas e respostas ad hoc às vulnerabilidades divulgadas. Esta abordagem funciona num ambiente de ameaça em que o tempo permite que a descoberta de vulnerabilidades permaneça gerível. No entanto, com um aumento do volume de vulnerabilidades, as práticas atuais podem tornar-se insuficientes para manter a resiliência operacional.

(7) Este aumento do volume também expõe os atuais processos de correção a sobrecarga, uma vez que dão prioridade a medidas de correção com base no risco e exigem testes das correções de software (*patches*) antes da sua execução, a fim de assegurar a estabilidade operacional. Se forem detetadas demasiadas vulnerabilidades com impacto crítico num curto espaço de tempo, de modo a aumentar substancialmente o número de correções críticas de software necessárias, as instituições financeiras podem ter de decidir entre deixar-se expostas a riscos cibernéticos significativos ou reduzir os requisitos de testes de correções (*patch-testing*), correndo assim o risco de incidentes e interrupções operacionais.

([1]) JO L 1 de 3.1.1994, p. 3, ELI: http://data.europa.eu/eli/agree_internation/1994/1/oj.
([2]) JO L 331 de 15.12.2010, p. 1, ELI: http://data.europa.eu/eli/reg/2010/1092/oj.
([3]) JO C 58 de 24.2.2011, p. 4.

(8) Antes, o desenvolvimento de explorações de vulnerabilidades (*exploits*) convertidas em arma era, em grande de medida, feito manualmente e levava dias ou semanas a ser realizado por peritos humanos, ao passo que, atualmente, aquele desenvolvimento pode ser feito pelos FAIM em minutos ou horas. Tal constitui um colapso das margens de tempo defensivas, que são necessárias para manter a continuidade de funções críticas e importantes durante a correção.

(9) Com a proliferação de explorações de vulnerabilidades convertidas em arma, correspondentes a vulnerabilidades críticas impulsionadas pela IA, e a consequente redução das margens de tempo defensivas, o risco para funções críticas ou importantes e para as instituições aumenta acentuadamente. Se esses riscos se materializarem em simultâneo nessas funções e instituições, tal poderá resultar num aumento permanente do ciber-risco sistémico para o qual, atualmente, não existe um quadro de mitigação plenamente eficaz. Devido à forte interligação no setor financeiro da União, bem como entre esse setor e outros setores e jurisdições, esta situação representa um risco sistemático e tem potencial para criar fragilidades sistémicas.

(10) Além disso, os FAIM estão atualmente a ser desenvolvidos por apenas um pequeno número de fornecedores de IA, vários dos quais manifestaram preocupação quanto ao facto de os futuros FAIM poderem ser demasiado poderosos para um acesso público sem restrições.

(11) A IA já está a ser utilizada por atores maliciosos para reforçar os ciberataques. É provável que esses intervenientes acabem por obter, através de fugas, furto, desenvolvimento independente ou acesso aberto, modelos de IA com capacidades comparáveis às atualmente implantadas em contextos defensivos controlados.

(12) Embora os FAIM possam aumentar significativamente as capacidades ofensivas e a probabilidade de ciberataques sofisticados, também reforçarão as capacidades defensivas, especificamente no que diz respeito à descoberta de vulnerabilidades, correlação de dados e medidas corretivas por parte de instituições individuais. No entanto, a curto e médio prazo, é provável que o aumento da velocidade, da escala e da exatidão das capacidades ofensivas supere os benefícios.

(13) O rápido desenvolvimento dos FAIM torna necessário abordar sem demora os riscos identificados para a estabilidade financeira para evitar a sua concretização ou, pelo menos, atenuar o seu potencial impacto. A fim de assegurar a estabilidade financeira nos mercados financeiros da União, todos os membros do Comité Europeu do Risco Sistémico (CERS) devem ter em conta as implicações dos FAIM na capacidade operacional e na resiliência das instituições financeiras no contexto das suas medidas de política macroprudencial e microprudencial. Isto sem prejuízo dos mandatos de política monetária dos bancos centrais da União. A título de exemplo, e entre outras iniciativas em curso de outras autoridades, o BCE, no seu papel de autoridade de supervisão bancária, solicitou às instituições significativas que avaliassem, sem demora, o impacto da evolução do panorama de ameaças e que, até 31 de outubro de 2026, desenvolvessem um plano de ação abrangente que defina medidas concretas destinadas a fazer face a esses riscos ([4]).

(14) À medida que a tecnologia de IA prolifera, é importante assegurar que todas as infraestruturas críticas e, em especial, as instituições financeiras, estejam preparadas para enfrentar ciberataques impulsionados por FAIM e façam preparativos atempados e adequados. No entanto, esses esforços defensivos por parte de entidades individuais seriam insuficientes. Uma resposta eficaz e a atenuação dos riscos exigem uma resposta coordenada que envolva todas as partes afetadas, incluindo os fornecedores de IA, os fornecedores de software, as empresas de segurança, os responsáveis pela manutenção de código-fonte aberto, as instituições financeiras e as autoridades, tanto a nível nacional como da União.

(15) Ao abordar as questões acima referidas, é importante recordar os quadros jurídicos e políticos pertinentes da União, em especial o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho ([5]), o Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho ([6]), o Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho ([7]) e a Recomendação do Comité Europeu do Risco Sistémico (CERS/2021/17) ([8]).

([4]) A carta dirigida às instituições significativas está disponível no sítio *Web* do BCE dedicado à supervisão bancária em www.bankingsupervision.europa.eu.

([5]) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Recomendação do Comité Europeu do Risco Sistémico, de 2 de dezembro de 2021, sobre um quadro pan-europeu de coordenação para as autoridades competentes relativo a ciberincidentes sistémicos (CERS/2021/17) (JO C 134 de 25.3.2022, p. 1).

(16) O Regulamento (UE) 2022/2554 estabelece um quadro abrangente para as instituições financeiras identificarem, gerirem, monitorizarem e mitigarem os riscos associados às TIC, incluindo os riscos decorrentes de ciberataques. Dada a interligação do setor financeiro e a sua dependência de sistemas de TIC e de terceiros prestadores de serviços, um ciberataque bem-sucedido que afete uma ou mais instituições financeiras ou os seus prestadores de serviços críticos poderá ter implicações sistémicas significativas. As autoridades de supervisão financeira deverão dar a devida prioridade às atividades de supervisão neste domínio, tendo em conta o potencial impacto desses ciberataques na estabilidade, integridade e fiabilidade do sistema financeiro, bem como os danos operacionais, financeiros e para os consumidores que daí possam resultar.

(17) O Regulamento (UE) 2024/1689 estabelece regras harmonizadas para a colocação no mercado, a colocação em serviço e a utilização de sistemas de IA e modelos de IA de finalidade geral na União, incluindo, em determinadas circunstâncias, sistemas e modelos fornecidos por prestadores de IA estabelecidos em países terceiros em que o resultado produzido pelo sistema de IA é utilizado na União ou em que um modelo de IA está integrado num sistema colocado no mercado da União. Este regulamento prevê igualmente regras específicas, incluindo um regime regulamentar mais rigoroso, para os modelos classificados como modelos de IA de finalidade geral com risco sistémico.

(18) O Regulamento (UE) 2024/2847 introduz requisitos de cibersegurança obrigatórios para os fabricantes, que abrangem o planeamento, a conceção, o desenvolvimento e a manutenção de produtos de hardware e software com elementos digitais colocados no mercado da União. Exige igualmente que os fabricantes corrijam as vulnerabilidades durante o ciclo de vida dos seus produtos. Assim que for plenamente aplicável, em dezembro de 2027, as entidades financeiras que colocam esses produtos no mercado da União terão também de assegurar que esses produtos cumprem esses requisitos.

(19) A Recomendação CERS/2021/17 recomendou o desenvolvimento, pelas Autoridades Europeias de Supervisão (AES), conjuntamente através do Comité Conjunto e em conjunto com o Banco Central Europeu (BCE), o CERS e as autoridades nacionais competentes, de uma resposta coordenada eficaz a nível da União em caso de ciberincidentes transfronteiriços graves ou ameaças conexas que possam ter um impacto sistémico no setor financeiro da União. Tal resultou na criação do quadro pan-europeu de coordenação de ciberincidentes sistémicos (*pan-European Systemic Cyber Incident Coordination Framework* — EU-SCICF), que proporciona uma plataforma valiosa e operacional para o intercâmbio de informações e a coordenação entre as autoridades financeiras.

(20) Neste contexto, o CERS adota um alerta de natureza geral para fazer face aos riscos significativos para a estabilidade financeira amplificados pelo desenvolvimento de FAIM. O alerta tem em conta o trabalho analítico realizado na nota do CERS intitulada «*Addressing Frontier AI Models with cyber capabilities from a financial stability perspetive*», publicada em junho de 2026 ([9]),

ADOTOU O PRESENTE ALERTA:

SECÇÃO 1

Alerta

Novo cenário de risco

O rápido desenvolvimento de modelos de IA de fronteira com cibercapacidades introduz alterações significativas no cenário de risco para o sistema financeiro da União. Os dados atuais indicam que os FAIM são capazes de detetar vulnerabilidades, gerando explorações de vulnerabilidades operacionais (*exploits*) e executando de forma autónoma ciberataques em grande escala a uma velocidade, escala e nível de exatidão muito superiores aos dos modelos de IA anteriores. Isto constitui uma mudança de paradigma no domínio da cibersegurança e de um ponto de inflexão em termos de capacidade de IA.

O CERS considera que estes desenvolvimentos são uma fonte de riscos sistémicos para o sistema financeiro, com potencial para gerar efeitos adversos significativos na cibersegurança através da descoberta acelerada de vulnerabilidades, da redução do tempo disponível para uma resposta e uma defesa eficazes, do aumento da escala e da sofisticação dos ciberataques e da introdução de novas dependências e riscos de concentração no sistema financeiro. Embora o CERS reconheça as capacidades defensivas reforçadas que os FAIM oferecerão às instituições financeiras, é provável que estas capacidades se concretizem gradualmente ao longo dos próximos anos, exigindo que as instituições financeiras operem durante um período de transição caracterizado por um risco elevado, grande incerteza e um panorama tecnológico em rápida evolução. Dada a natureza altamente digitalizada e interligada do sistema financeiro, esses efeitos adversos na cibersegurança podem propagar-se rapidamente, afetando funções críticas e importantes em todas as instituições financeiras, conduzindo, em última análise, a perturbações sistémicas e à perda de confiança no sistema financeiro.

([9]) Disponível (em inglês) no sítio *web* do CESR em www.esrb.europa.eu.

Os FAIM emergentes aumentam o risco inerente às TIC, conduzindo a uma menor resiliência operacional em todo o setor financeiro, em especial em quatro domínios: a) tempo, incluindo a capacidade de aplicar rapidamente correções (*patches*) a sistemas complexos sem causar falhas operacionais, tendo em conta o desaparecimento de margens de tempo defensivas entre a descoberta de vulnerabilidades e a conversão em arma destas explorações de vulnerabilidades; b) a capacidade dos defensores, incluindo a sua aptidão para realizar testes de segurança, automatizados e manuais, assistidos por FAIM, bem como a sua capacidade para proteger, detetar e responder a ameaças decorrentes do uso adversário de FAIM; c) concentração, incluindo a dependência de um número limitado de fornecedores de IA, que, por sua vez, dependem de prestadores de serviços de computação em nuvem, componentes de código-fonte aberto e outros programas informáticos amplamente utilizados; e d) a capacidade das autoridades, incluindo a sua calibração das expectativas, a realização de testes de esforço e medidas de preparação em conformidade com a evolução dos FAIM, de modo a que as falhas operacionais não se tornem uma fonte de instabilidade mais generalizada.

Além disso, é difícil estabelecer e manter a visibilidade sobre a implantação da IA em qualquer instituição financeira — incluindo compreender plenamente onde e como a IA é implantada — tendo em conta que é utilizada em interfaces de clientes, agentes internos, processos empresariais e integração com terceiros.

Avaliação sistémica

Os desenvolvimentos identificados podem alterar substancialmente tanto a escala como a estrutura do ciber-risco, aumentando os riscos diretos e indiretos para a estabilidade financeira. As capacidades dos FAIM podem colocar os quadros de resiliência existentes sob uma pressão substancial, especialmente se os incidentes forem generalizados e ocorrerem em simultâneo. Os incidentes podem também propagar-se rapidamente entre as instituições e os mercados financeiros se forem afetados prestadores terceiros críticos, ecossistemas tecnológicos partilhados ou componentes de código-fonte aberto amplamente utilizados, aumentando o risco de perturbações conexas com implicações sistémicas.

Os FAIM alteram três fontes de assimetria no setor financeiro: a primeira entre jurisdições, a segunda entre defensores e atacantes e a terceira entre instituições financeiras mais dotadas de recursos e as menos equipadas.

Em primeiro lugar, a atual concentração geográfica dos principais fornecedores de IA fora da União deixa a União exposta à dependência estratégica e a riscos geopolíticos. Para atenuar a assimetria do conhecimento e da tecnologia entre jurisdições, é necessário adotar medidas para facilitar o acesso adequado e proporcionado da União e dos seus Estados-Membros aos FAIM recentemente desenvolvidos. Essas medidas deverão ser oportunas, coerentes e eficientes, tanto em termos de política como de execução, e deverão ter devidamente em conta os diferentes setores financeiros da União, beneficiando dos conhecimentos especializados das AES. Tal atenuará não só uma assimetria entre a União e as jurisdições de países terceiros, mas também entre as instituições financeiras estabelecidas em diferentes Estados-Membros, preservando condições de concorrência equitativas dentro e fora da União e minimizando o risco sistémico. Acordos que facilitem o acesso aos FAIM apenas para determinadas categorias de instituições ou em jurisdições selecionadas contribuiriam para a fragmentação do mercado único do financiamento, reduzindo a sua liquidez e profundidade.

Em segundo lugar, no que diz respeito à assimetria entre atacantes e defensores, os FAIM reduzem o custo de entrada para os atacantes. É provável que os autores das ameaças dependam cada vez mais das FAIM para realizar as partes mais avançadas do ponto de vista técnico e com grande intensidade de mão de obra das operações ofensivas, reduzindo os custos. Em contrapartida, os defensores estão limitados por requisitos operacionais, dependências e obrigações regulamentares, o que limita o efeito e a escala em que podem beneficiar dos FAIM a curto e médio prazo, exigindo, em última análise, períodos mais longos para se adaptarem.

Em terceiro lugar, existem diferenças na forma como as instituições financeiras dispõem de recursos e estão equipadas para enfrentar os desafios colocados pelos FAIM. Estas diferenças podem ser causadas por custos que são fixos em vez de escaláveis, por limitações de recursos e por um acesso limitado a especialistas. Quando existe assimetria na capacidade de fazer face a esses desafios, o elo mais fraco da cadeia pode afetar a estabilidade do sistema.

Implicações

É essencial assegurar que os sistemas de pagamentos e de liquidação e as infraestruturas do mercado financeiro sistemicamente importantes continuem a estar protegidos contra as vulnerabilidades decorrentes da utilização e do desenvolvimento de FAIM. Os operadores públicos e privados devem rever e atualizar exaustivamente os seus quadros de cibersegurança, para ter em conta essas vulnerabilidades. As autoridades responsáveis pela supervisão ou superintendência devem adotar medidas para assegurar que os sistemas são adequadamente protegidos. A cooperação entre as autoridades e as instituições financeiras privadas deverá ser prosseguida sempre que necessário para aumentar a segurança e a resiliência do sistema financeiro da União.

No seu relatório de 2020 sobre o ciber-risco sistémico ([10]), o CERS identificou a velocidade, a escala e a intenção maliciosa das ciberameaças como possíveis fontes de propagação de risco sistémico. As autoridades devem estar cientes de que embora os FAIM representem uma nova fonte de propagação, eles também amplificam as fontes anteriormente identificadas, e devem integrar este conhecimento na sua ação política. Tendo em conta todos os riscos para a estabilidade financeira decorrentes da exposição operacional ao risco cibernético no setor financeiro, é importante assegurar que as preocupações identificadas no presente alerta sejam refletidas no trabalho de supervisão e superintendência e nas posições políticas adotadas pelas autoridades relevantes, no âmbito dos respetivos mandatos.

As autoridades competentes, no âmbito das respetivas competências e especificamente ao abrigo do quadro estabelecido pelo Regulamento (UE) 2022/2554, devem estar cientes das três fontes de assimetria anteriormente mencionadas, introduzidas pelos FAIM no setor financeiro. Para de reduzir estas assimetrias, devem ser considerados acordos de cooperação e coordenação setorial, juntamente com os quadros de teste existentes ([11]). As autoridades financeiras devem também assegurar que os conselhos de administração das instituições financeiras privadas estão plenamente empenhados em mitigar os riscos cibernéticos impulsionados pelos FAIM, que existem quadros claros de governação e responsabilização e que as respostas atempadas são adequadamente planeadas, juntamente com os correspondentes investimentos internos.

Vários desenvolvimentos possíveis considerados neste alerta — seja o impacto sistémico, o risco geopolítico ou a alteração do equilíbrio entre atacantes e defensores — têm potencial para afetar o funcionamento do sistema financeiro e a confiança no mesmo. Para os avaliar continuamente, o CERS terá em conta a necessidade de refletir essa evolução em avaliações de risco, nos quadros de teste e nas expectativas de supervisão, bem como no desenvolvimento de cenários futuros. O CERS monitorizará igualmente a utilização e o desenvolvimento dos FAIM e o seu impacto no setor financeiro do ponto de vista do risco sistémico. Além disso, o CERS reavaliará a evolução em cada avaliação trimestral de risco ao nível do Conselho Geral e ponderará outras ações, quando necessário.

SECÇÃO 2

Definições

Para efeitos do presente alerta, entende-se por:

1) «Prestador de IA», um prestador na aceção do artigo 3.º, ponto 3), do Regulamento (UE) 2024/1689;

2) «Modelos de IA de fronteira (*Frontier AI Models* — FAIM)», modelos avançados de IA de finalidade geral capazes de afetar substancialmente ciberoperações ofensivas ou defensivas;

3) «Ciberataque», um ciberataque na aceção do artigo 1.º do Regulamento (UE) 2019/796 do Conselho ([12]), incluindo quando proveniente do interior da União;

4) «Vulnerabilidade», uma vulnerabilidade na aceção do artigo 3.º, ponto 16), do Regulamento (UE) 2022/2554;

5) «Exploração de vulnerabilidades (*exploit*)», uma ferramenta, técnica ou método utilizado para tirar partido de uma ou mais vulnerabilidades para obter acesso não autorizado aos sistemas, modificá-los, perturbá-los ou, de qualquer outro modo, dar origem a riscos no domínio das TIC ou a incidentes relacionados com as TIC;

6) «Conversão em arma», a preparação ou adaptação de explorações de vulnerabilidades que permitam a exploração sistemática ou escalável de vulnerabilidades;

7) «Função crítica ou importante»», uma função crítica ou importante na aceção do artigo 3.º, ponto 22), do Regulamento (UE) 2022/2554;

8) «Modelo de IA de finalidade geral», um modelo de IA de finalidade geral na aceção do artigo 3.º, ponto 63), do Regulamento (UE) 2024/1689;

9) «Modelo de IA de finalidade geral com risco sistémico», um modelo de IA de finalidade geral classificado como apresentando risco sistémico nos termos do artigo 51.º, n.º1, do Regulamento (UE) 2024/1689;

10) «Incidente relacionado com as TIC», um incidente relacionado com as TIC na aceção do artigo 3.º, ponto 8), do Regulamento (UE) 2022/2554;

([10]) Ver «*Systemic cyber risk*», CERS, fevereiro de 2020, disponível (em inglês) no sítio *web* do CERS em www.esrb.europa.eu.

([11]) Por exemplo, TIBER (do inglês, *Threat Intelligence based Ethical Red teaming*), testes de penetração baseados em ameaças (*threat-led penetration testing* — TLPT), equipas avançadas de simulação de ataques (*advanced red teaming* — ART) e testes de esforço de ciber--resiliência (*cyber resilience stress testing* — CyRST).

([12]) Regulamento (UE) 2019/796 do Conselho, de 17 de maio de 2019, relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros (JO L 129 I de 17.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11) «Risco associado às TIC», um risco associado às TIC na aceção do artigo 3.º, ponto 5), do Regulamento (UE) 2022/2554;

12) «Resiliência operacional», resiliência operacional digital na aceção do artigo 3.º, ponto 1), do Regulamento (UE) 2022/2554;

Feito em Frankfurt am Main, em 25 de junho de 2026.

O Chefe do Secretariado do CERS

Em nome do Conselho Geral do CERS,

Francesco MAZZAFERRO