Conselho
da União Europeia

Bruxelas, 22 de janeiro de 2026
(OR. en)

5611/26
ADD 2

Dossiês interinstitucionais:
2026/0011 (COD)
2026/0012 (COD)

CYBER 29
JAI 85
DATAPROTECT 22
TELECOM 29
MI 58
IND 48
CADREFIN 26
FIN 100
BUDGET 3
CODEC 90

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	21 de janeiro de 2026
para:	Thérèse BLANCHET, secretária-geral do Conselho da União Europeia
n.° doc. Com.:	SWD(2026) 12 final
Assunto:	DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO RESUMO DO RELATÓRIO DA AVALIAÇÃO DE IMPACTO que acompanha o documento Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à Agência da União Europeia para a Cibersegurança (ENISA), ao enquadramento europeu para a certificação da cibersegurança e à segurança da cadeia de abastecimento de TIC e que revoga o Regulamento (UE) 2019/881 (Regulamento Cibersegurança 2) e Proposta de Diretiva do Parlamento Europeu e do Conselho que altera a Diretiva (UE) 2022/2555 no respeitante a medidas de simplificação e ao alinhamento com a [proposta de Regulamento Cibersegurança 2]

Envia-se em anexo, à atenção das delegações, o documento SWD(2026) 12 final.

Anexo: SWD(2026) 12 final

COMISSÃO
EUROPEIA

Estrasburgo, 20.1.2026
SWD(2026) 12 final

DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO

RESUMO DO RELATÓRIO DA AVALIAÇÃO DE IMPACTO

que acompanha o documento

Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à Agência da União Europeia para a Cibersegurança (ENISA), ao enquadramento europeu para a certificação da cibersegurança e à segurança da cadeia de abastecimento de TIC e que revoga o Regulamento (UE) 2019/881 (Regulamento Cibersegurança 2)

e

Proposta de Diretiva do Parlamento Europeu e do Conselho que altera a Diretiva (UE) 2022/2555 no respeitante a medidas de simplificação e ao alinhamento com a [proposta de Regulamento Cibersegurança 2]

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

Resumo da avaliação de impacto

Objetivo

O principal objetivo da presente avaliação de impacto é avaliar a adequação da regulamentação em vigor para fazer face à evolução das ameaças à cibersegurança em toda a UE. A avaliação propõe um conjunto integrado de opções estratégicas destinadas a reforçar a Agência da União Europeia para a Cibersegurança (ENISA), reformar o enquadramento europeu para a certificação da cibersegurança e simplificar a conformidade com o atual quadro legislativo relativo à cibersegurança. Esta avaliação sublinha a importância de modular a cibergovernação para a harmonizar com os avanços tecnológicos e as exigências do mercado, assegurando simultaneamente a competitividade e tendo os impactos ambientais em conta.

Descrição do problema

Apesar dos esforços em curso, o panorama da cibersegurança da UE continua a enfrentar desafios significativos num contexto de ameaças cada vez mais complexas. A coordenação insuficiente entre os Estados-Membros e outros intervenientes a nível da UE, a estagnação da aplicação dos instrumentos políticos e os obstáculos e a complexidade regulamentares inibem a gestão eficiente da cibersegurança. Estas questões resultam num aumento dos custos para as empresas e as autoridades públicas, no aumento dos riscos de ciberincidentes e em níveis heterogéneos de proteção dos cidadãos.

Fundamentação da ação da UE

As ameaças à cibersegurança transcendem as fronteiras nacionais, pelo que uma abordagem unificada é vital para uma resposta sólida. Uma intervenção a nível da UE assegura uma proteção coerente, reforça a competitividade ao proporcionar condições de concorrência equitativas e facilita a livre circulação de serviços e produtos digitais no mercado único. A harmonização a nível da UE também reduz os encargos administrativos graças à simplificação da conformidade e à racionalização dos procedimentos.

Opções estratégicas e opções preferidas

O presente relatório analisa quatro domínios de intervenção, cada um com um conjunto de opções estratégicas consideradas à luz dos objetivos específicos a alcançar: 1) mandato da ENISA (também faz parte do atual Regulamento Cibersegurança); 2) enquadramento europeu para a certificação da cibersegurança (também faz parte do atual Regulamento Cibersegurança) e 3) alterações específicas da Diretiva SRI 2 que visam a simplificação, estando simultaneamente interligadas ao mandato da ENISA e ao enquadramento europeu para a certificação da cibersegurança. Cada um destes conjuntos de opções constitui, por si só, um domínio de intervenção; simultaneamente, está interligado aos demais e é pertinente para a sua aplicação.

Opções para fazer face ao desfasamento entre o quadro estratégico da UE relativo à cibersegurança e as necessidades das partes interessadas num ambiente cada vez mais hostil

Opção A.1: *clarificar o mandato da ENISA e estabelecer prioridades* — esta opção asseguraria um quadro claro e estável para as funções da ENISA, incorporando as atribuições definidas por outros atos legislativos.

Opção A.2: *reformar o mandato da ENISA* — esta opção revogaria e substituiria o Regulamento Cibersegurança, procedendo a uma revisão do mandato da agência.

Opção A.3: *reformar o mandato da ENISA com uma forte ênfase no apoio operacional* — esta opção basear-se-ia na opção A.2. Além disso, a ENISA desenvolveria capacidades para apoiar diretamente as entidades abrangidas pela Diretiva SRI 2 na resposta a um incidente de cibersegurança e na recuperação do mesmo, a pedido de um Estado-Membro.

Opções para o enquadramento europeu para a certificação da cibersegurança

Opção B.1: *clarificar o âmbito, os elementos e os objetivos do enquadramento europeu para a certificação da cibersegurança e introduzir um mecanismo de manutenção* — esta opção preverá um novo mecanismo de manutenção dos sistemas, após a sua adoção, a executar pela ENISA.

Opção B.2: *reformar o enquadramento europeu para a certificação da cibersegurança por meio da revisão dos seus procedimentos e do alargamento do seu âmbito a fim de facilitar a simplificação da conformidade regulamentar* — nesta opção, o Regulamento Cibersegurança seria revogado e substituído por um novo regulamento. Além do proposto na opção B.1, seriam revistos os procedimentos relacionados com o pedido, o desenvolvimento e a adoção de sistemas de modo a melhorar a responsabilização e a eficiência.

Opção B.3: *reformar o enquadramento europeu para a certificação da cibersegurança, tal como previsto na opção B.2, e introduzir uma certificação obrigatória da postura de cibersegurança* — esta opção basear-se-ia na opção B.2, visando reforçar ainda mais o impacto do enquadramento mediante a introdução de uma certificação obrigatória para as entidades essenciais abrangidas pela Diretiva SRI 2, tendo em conta cenários de risco específicos, em vez de ter exclusivamente como base a certificação voluntária das entidades.

Opções para simplificação

Opção C.1: *adotar uma abordagem não vinculativa e não legislativa, incluindo o recurso a habilitações existentes (adoção de atos de execução nos termos do artigo 21.º, n.º 5, e do artigo 23.º, n.º 11, da Diretiva SRI 2)* — esta opção prevê a adoção de atos de execução ao abrigo das habilitações existentes da Diretiva SRI 2 a fim de assegurar um maior grau de harmonização das medidas de gestão dos riscos de cibersegurança, dos limiares de notificação de incidentes e das informações, formatos e procedimentos de notificação, juntamente com a adoção de um conjunto de orientações para reforçar a segurança jurídica e a harmonização da aplicação.

Opção C.2: *intervenção específica tendo em vista uma maior simplificação da conformidade com o quadro legislativo da União relativo à cibersegurança* — esta opção implica uma intervenção limitada por meio de alterações do Regulamento Cibersegurança e da Diretiva SRI 2 destinadas a simplificar aspetos específicos do quadro de cibersegurança, incluindo adaptações do âmbito de aplicação, harmonização máxima dos atos de execução, prova de conformidade por via da certificação e adoção do conjunto de orientações previsto na opção C.1.

Opção C.3: *harmonização das medidas relacionadas com a cibersegurança estabelecidas na legislação da União* — esta opção basear-se-ia na opção C.2 e eliminaria todas as medidas de gestão dos riscos de cibersegurança ou as habilitações relacionadas com as mesmas constantes da legislação setorial. Em vez disso, o ecossistema da Diretiva SRI 2 seria alterado de modo a prever requisitos simplificados para todos os tipos de entidades, assegurando assim uma maior harmonização.

Opções para a segurança da cadeia de abastecimento de TIC

Opção D.1: *adotar uma abordagem não vinculativa para fazer face aos riscos de cibersegurança nas cadeias de abastecimento de TIC* — esta opção não prevê uma intervenção regulamentar a nível da UE. Em vez disso, a Comissão aumentaria o número de avaliações coordenadas dos riscos e de conjuntos de instrumentos voluntários.

Opção D.2: *intervenção regulamentar* ad hoc *que codifica o conjunto de instrumentos para as redes 5G* — esta opção codificaria as medidas do conjunto de instrumentos para as redes 5G. Introduziria a obrigação de os Estados-Membros assegurarem que não sejam utilizados componentes de fornecedores de alto risco nos principais ativos da rede.

Opção D.3: *quadro abrangente e horizontal para fazer face aos riscos de cibersegurança nas cadeias de abastecimento de TIC* — esta opção estabeleceria um quadro regulamentar horizontal neutro do ponto de vista tecnológico e setorial para fazer face aos riscos de cibersegurança não técnicos nas cadeias de abastecimento de TIC.

Após análises exaustivas, o pacote de medidas preferido inclui as seguintes opções: opção A.2 — reformar o mandato da ENISA; opção B.2 — reformar o enquadramento europeu para a certificação da cibersegurança por meio da revisão dos seus procedimentos e do alargamento do seu âmbito a fim de facilitar a simplificação da conformidade regulamentar; opção C.2 — intervenção específica tendo em vista uma maior simplificação da conformidade com o quadro legislativo da União relativo à cibersegurança e opção D.3 — quadro abrangente e horizontal para fazer face aos riscos de cibersegurança das cadeias de abastecimento de TIC.

Esta combinação oferece uma resposta equilibrada aos desafios políticos identificados, reforçando significativamente a eficácia, a eficiência e a coerência em toda a União.

Principais impactos

Análise custo-benefício: a transição para o quadro regulamentar proposto implicará custos tanto para a ENISA, estimados num máximo de 161,3 milhões de EUR ao longo de cinco anos para cumprir as suas novas atribuições, como para as autoridades públicas em toda a UE, estimados num máximo de 80 milhões de EUR ao longo de cinco anos para efeitos de supervisão (tendo em conta as poupanças de custos pertinentes). No que diz respeito às empresas, durante um período de transição de três anos, a eliminação progressiva de equipamentos específicos de alto risco poderia conduzir a custos anuais de 3,4 a 4,3 mil milhões de EUR para os operadores de redes móveis, ao passo que os investimentos em fornecedores de confiança poderiam aumentar simultaneamente até 2 mil milhões de EUR por ano. Além disso, espera-se que a racionalização e a redução das obrigações de conformidade promovam poupanças de custos para as empresas que poderão chegar aos 14,6 mil milhões de EUR. Ademais, a melhoria geral da postura de cibersegurança e da soberania tecnológica da UE e o estímulo à inovação e à competitividade, que, a longo prazo, deverão compensar amplamente as despesas iniciais, trariam benefícios significativos aos cidadãos, às autoridades públicas e às empresas.

Competitividade: ao reduzir a fragmentação do mercado e harmonizar a regulamentação, as opções preferidas reforçam a igualdade concorrencial em toda a UE, proporcionando às empresas vias mais claras para o cumprimento e a inovação.

Verificação da coerência climática: a avaliação teve em conta o potencial impacto ambiental de cada opção. Foi dada especial atenção à eficiência energética, às emissões relacionadas com viagens e à consolidação das infraestruturas. Das opções preferidas, as opções A.2, B.2 e C.2 têm um impacto ambiental limitado, ao passo que a opção D.3 prevê a neutralidade ambiental, tendo em conta o ciclo de vida dos produtos e períodos de transição para a substituição dos principais ativos. Estas considerações estão em consonância com o compromisso da UE para com a sustentabilidade.

Digital como regra: a ênfase na racionalização dos processos digitais demonstra o empenho da UE numa abordagem que prioriza o digital, assegurando um intercâmbio de dados e uma tomada de decisões mais rápidos e fiáveis. A opção D.3 poderia também ter um impacto elevado na digitalização, uma vez que implicaria a substituição de componentes de entidades estabelecidas em países terceiros que suscitam preocupações no que diz respeito à cibersegurança ou de entidades controladas por entidades desses países terceiros.

Simplificação e redução de encargos: as opções preferidas contribuem para a simplificação graças à introdução de clarificações do âmbito e de medidas para racionalizar a conformidade e a supervisão, reduzindo os encargos administrativos. O princípio do «entra um, sai um» é tido em conta ao assegurar que as novas obrigações são compensadas por reduções noutras áreas.

Conclusão

A presente avaliação de impacto apresenta uma estratégia abrangente para reforçar a cibersegurança da UE, resolver ineficiências regulamentares e preparar o panorama digital para futuros desafios. Recomenda uma abordagem colaborativa e coesa que baseia as reformas políticas nos quadros existentes, adaptando-se simultaneamente a novas realidades tecnológicas. Com estas medidas, a UE visa assegurar uma economia digital resiliente, competitiva e sustentável.