Consejo de la Unión Europea

Bruselas, 22 de enero de 2026
(OR. en)

5611/26
ADD 2

Expedientes interinstitucionales:
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 TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	21 de enero de 2026
A:	D.ª Thérèse BLANCHET, secretaria general del Consejo de la Unión Europea
N.° doc. Ción.:	SWD(2026) 12 final
Asunto:	DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN RESUMEN DEL INFORME DE LA EVALUACIÓN DE IMPACTO que acompaña a los documentos Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el marco europeo de certificación de la ciberseguridad y la seguridad de las cadenas de suministro de TIC y por el que se deroga el Reglamento (UE) 2019/881 («Reglamento sobre la Ciberseguridad 2») Y Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2022/2555 sobre medidas de simplificación y armonización con la [Propuesta de Reglamento sobre la Ciberseguridad 2]

Adjunto se remite a las delegaciones el documento SWD(2026) 12 final.

Adj.: SWD(2026) 12 final

COMISIÓN
EUROPEA

Estrasburgo, 20.1.2026
SWD(2026) 12 final

DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN

RESUMEN DEL INFORME DE LA EVALUACIÓN DE IMPACTO

que acompaña a los documentos

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el marco europeo de certificación de la ciberseguridad y la seguridad de las cadenas de suministro de TIC y por el que se deroga el Reglamento (UE) 2019/881 («Reglamento sobre la Ciberseguridad 2»)

Y

Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2022/2555 sobre medidas de simplificación y armonización con la [Propuesta de Reglamento sobre la Ciberseguridad 2]

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

Resumen de la evaluación del impacto

Objetivo

El objetivo principal de esta evaluación de impacto es evaluar la adecuación de la normativa vigente para hacer frente a la evolución de las ciberamenazas en la UE. Propone un conjunto integrado de opciones de actuación destinadas a reforzar la Agencia de la Unión Europea para la Ciberseguridad (ENISA), reformar el marco europeo de certificación de la ciberseguridad y simplificar el cumplimiento del marco legislativo vigente en materia de ciberseguridad. Esta evaluación pone de relieve la importancia de modular la gobernanza cibernética para armonizarla con los avances tecnológicos y las demandas del mercado, garantizando al mismo tiempo la competitividad y teniendo en cuenta el impacto medioambiental.

Descripción del problema

A pesar de los esfuerzos que se están realizando, la ciberseguridad de la UE sigue enfrentándose a retos significativos en un contexto de amenazas cada vez más complejas. La coordinación insuficiente entre los Estados miembros y otros agentes a nivel de la UE y el estancamiento en la aplicación de las herramientas de actuación, unidos a las trabas y la complejidad normativas, dificultan una gestión eficiente de la ciberseguridad. Estas cuestiones se traducen en un aumento de los costes para las empresas y las autoridades públicas y en un mayor riesgo de incidentes de ciberseguridad, así como en niveles desiguales de protección de los ciudadanos.

Justificación de la acción de la UE

Las ciberamenazas trascienden las fronteras nacionales; por lo tanto, un enfoque unificado es vital para poder proporcionar una respuesta sólida. Una intervención a nivel de la UE ofrece una protección coherente, mejora la competitividad gracias a unas condiciones de competencia equitativas y facilita la libre circulación de servicios y productos digitales en el mercado único. La armonización a escala de la UE también reduce las cargas administrativas, al simplificar el cumplimiento y racionalizar los procedimientos.

Opciones de actuación y opción preferida

El presente informe analiza cuatro ámbitos de intervención, cada uno de ellos con un conjunto de opciones de actuación consideradas en función de los objetivos específicos que deben alcanzarse: 1) mandato de ENISA (que también forma parte del actual Reglamento sobre la Ciberseguridad); 2) el marco europeo de certificación de la ciberseguridad (integrado también en el actual Reglamento sobre la Ciberseguridad) y 3) modificaciones específicas de la Directiva SRI 2 destinadas a simplificarla y, al mismo tiempo, vincularla con el mandato de ENISA y el marco europeo de certificación de la ciberseguridad. Cada uno de estos conjuntos de opciones representa un ámbito de intervención en sí mismo, y todos están interconectados y son pertinentes entre sí.

Opciones para abordar el desajuste entre el marco de actuación de la UE en materia de ciberseguridad y las necesidades de las partes interesadas en un contexto cada vez más hostil

Opción A.1: *Aclarar el mandato de ENISA y establecer prioridades* - Esta opción aportaría un marco claro y estable para las tareas de ENISA, ya que incorpora las tareas establecidas en otros actos legislativos.

Opción A.2: *Reformar el mandato de ENISA* - esta opción supondría derogar y sustituir el Reglamento sobre la Ciberseguridad y realizar una revisión completa del mandato de la Agencia.

Opción A.3: *Reformar el mandato de ENISA con un fuerte enfoque de apoyo operativo* - Esta opción se basaría en la opción A.2. Además, ENISA desarrollaría las capacidades necesarias para apoyar directamente a las entidades contempladas en la Directiva SRI 2 en su respuesta y recuperación ante incidentes de ciberseguridad cuando así lo solicite el Estado miembro.

Opciones para el marco europeo de certificación de la ciberseguridad

Opción B.1: *Aclarar el ámbito de aplicación, los elementos y los objetivos del marco europeo de certificación de la ciberseguridad e introducir un mecanismo de mantenimiento* - Esta opción proporcionará un nuevo mecanismo de mantenimiento de los esquemas, tras su adopción, que llevaría a cabo ENISA.

Opción B.2: *Reformar el marco europeo de certificación de la ciberseguridad revisando para ello sus procedimientos y ampliando su ámbito de aplicación para facilitar la simplificación del cumplimiento de la normativa* - Con arreglo a esta opción, el Reglamento sobre la Ciberseguridad sería derogado y sustituido por un nuevo reglamento. Además de la opción B.1, se revisaría el procedimiento relativo a la solicitud, el desarrollo y la adopción de esquemas para mejorar la responsabilidad pública y la eficiencia.

Opción B.3: *Reformar el marco europeo de certificación de la ciberseguridad según lo previsto en la opción B.2 e introducir la certificación obligatoria de la postura de ciberseguridad* - Esta opción se basaría en la opción B.2, pero su objetivo es seguir reforzando el impacto del marco mediante la introducción de la certificación obligatoria de las entidades esenciales contempladas por la Directiva SRI 2 teniendo en cuenta escenarios de riesgo específicos, en lugar de basarse únicamente en la certificación voluntaria de las entidades.

Opciones de simplificación

Opción C.1: *Adoptar un enfoque de instrumentos no vinculantes y no legislativos, incluido el uso de las habilitaciones existentes (adopción de actos de ejecución en virtud del artículo 21, apartado 5, y del artículo 23, apartado 11, de la Directiva SRI 2)* - Esta opción prevé la adopción de actos de ejecución en virtud de las habilitaciones previstas en la Directiva SRI 2 para garantizar un mayor grado de armonización de las medidas de gestión de riesgos de ciberseguridad y los umbrales de notificación de incidentes, así como la información, los

formatos y los procedimientos de notificación, junto con la adopción de un conjunto de directrices para mejorar la seguridad jurídica y la aplicación armonizada.

Opción C.2: *Intervención específica - mayor simplificación del cumplimiento del marco legislativo de la Unión pertinente en materia de ciberseguridad* - Esta opción implica una intervención limitada consistente en cambios en el Reglamento sobre la Ciberseguridad y la Directiva SRI 2 destinados a simplificar aspectos específicos del marco de ciberseguridad, como las adaptaciones del ámbito de aplicación, el máximo nivel de armonización posible de los actos de ejecución, la prueba de cumplimiento mediante la certificación y la adopción del conjunto de directrices previsto en la opción C1.

Opción C.3: *Armonización de las medidas relacionadas con la ciberseguridad establecidas en la legislación de la Unión* - Esta opción se basaría en la opción C.2 y eliminaría todas las medidas o habilitaciones para la gestión de riesgos de ciberseguridad con respecto a las incluidas en la legislación sectorial. En su lugar, el ecosistema de la Directiva SRI 2 se modificaría para establecer requisitos racionalizados para todos los tipos de entidades, en aras de una mayor armonización.

Opciones para la seguridad de las cadenas de suministro de TIC

Opción D.1: *Adoptar un enfoque no vinculante para abordar los riesgos de ciberseguridad para las cadenas de suministro de TIC* - Esta opción no contemplaría una intervención reguladora a nivel de la UE. la Comisión aumentaría el número de evaluaciones de riesgos coordinadas y de conjuntos de instrumentos voluntarios.

Opción D.2: *Intervención reguladora* ad hoc *para codificar el conjunto de instrumentos 5G.* Esta opción codificaría las medidas del conjunto de instrumentos 5G. Los Estados miembros tendrían la obligación de garantizar que los componentes de proveedores de alto riesgo no se utilizasen en activos clave de la red.

Opción D.3: *Marco integral y horizontal para abordar los riesgos de ciberseguridad de las cadenas de suministro de TIC* - Esta opción establecería un marco regulador horizontal, neutro en cuanto a tecnologías y sectores para abordar los riesgos de ciberseguridad no técnicos en las cadenas de suministro de TIC.

Tras amplios análisis, el paquete de actuaciones preferido incluye: Opción A.2: reformar el mandato de ENISA; opción B.2: reformar el marco europeo de certificación de la ciberseguridad revisando para ello el procedimiento y ampliando el ámbito de aplicación para facilitar la simplificación del cumplimiento de la normativa, y opción C.2: intervención específica – mayor simplificación del cumplimiento del marco legislativo pertinente de la Unión en materia de ciberseguridad, y opción D.3: marco integral y horizontal para abordar los riesgos de ciberseguridad de las cadenas de suministro de TIC.

Esta combinación ofrece una respuesta equilibrada a los retos de las políticas identificados y mejora notablemente la eficacia, la eficiencia y la coherencia en toda la UE.

Principales efectos

Análisis coste-beneficio: La transición al marco regulador propuesto generará costes a ENISA derivados del cumplimiento de sus nuevas tareas, los cuales se estima que ascenderán a hasta 161,3 millones EUR a lo largo de cinco años, así como a las autoridades públicas de toda la UE, por un importe de hasta 80 millones EUR a lo largo de cinco años, derivados de las tareas de supervisión (teniendo en cuenta los ahorros de costes oportunos). En cuanto a las empresas, durante un período de transición de 3 años, la eliminación progresiva de equipos específicos de alto riesgo podría dar lugar a unos costes anuales de entre 3 400 y 4 300 millones EUR para los operadores de redes móviles, mientras que las inversiones en proveedores de confianza podrían aumentar simultáneamente hasta 2 000 millones EUR al año. Además, se espera que la racionalización y la reducción de las obligaciones de cumplimiento generen una reducción en los costes para las empresas de hasta 14 600 millones EUR. Asimismo, los ciudadanos, las autoridades públicas y las empresas se beneficiarán notablemente de la mejora de la postura general de ciberseguridad de la UE y su soberanía tecnológica, además del fomento de la innovación y la competitividad, que se espera que compensen en gran medida los gastos iniciales a largo plazo.

Competitividad: Al reducir la fragmentación del mercado y armonizar la normativa, las opciones preferidas redundan en la igualdad competitiva en toda la UE, proporcionando a las empresas vías más claras de cumplimiento e innovación.

Control de la coherencia climática: En la evaluación se tuvo en cuenta el posible impacto ambiental de cada opción. Se prestó especial atención a la eficiencia energética, las emisiones relacionadas con los desplazamientos y la consolidación de las infraestructuras. Las opciones preferidas A.2, B.2 y C.2 tienen un impacto medioambiental limitado, mientras que D.3 incorpora la neutralidad medioambiental y tiene en cuenta el ciclo de vida de los productos y los períodos de transición para la sustitución de activos clave. Esto va en consonancia con el compromiso de la UE con la sostenibilidad.

Versión digital por defecto: El énfasis en procesos digitales racionalizados demuestra el compromiso de la UE con el enfoque «lo digital, primero» y aporta rapidez y fiabilidad al intercambio de datos y la toma de decisiones. La opción D.3 también tendría un gran impacto en la digitalización, ya que implicaría la sustitución de componentes de entidades establecidas en terceros países o controladas por entidades de terceros países que plantean preocupaciones en materia de ciberseguridad.

Simplificación y reducción de la carga: Las opciones preferidas contribuyen a la simplificación mediante la introducción de aclaraciones sobre el ámbito de aplicación y medidas para racionalizar el cumplimiento y la supervisión, reduciendo las cargas administrativas. Se adopta el principio de «una más, una menos», de manera que las nuevas obligaciones se compensan con menos obligaciones en otros ámbitos.

Conclusión

La presente evaluación de impacto ofrece una estrategia integral para mejorar la ciberseguridad de la UE, abordar las ineficiencias normativas y preparar el panorama digital para futuros retos. Recomienda un enfoque colaborativo y cohesivo, que base las reformas de

las políticas en los marcos existentes y se adapte al mismo tiempo a las nuevas realidades tecnológicas. A través de estas medidas, la UE pretende garantizar una economía digital resiliente, competitiva y sostenible.