Consejo de la Unión Europea

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

9399/26

Expedientes interinstitucionales:
2026/0011 (COD)
2026/0012 (COD)

LIMITE

CYBER 229
JAI 606
DATAPROTECT 161
TELECOM 239
MI 489
IND 342
CADREFIN 220
FIN 697
BUDGET 19
CSC 316
CODEC 937

NOTA

De:	Secretaría General del Consejo
A:	Comité de Representantes Permanentes/Consejo
Asunto:	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») 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] - Informe de situación

La Presidencia ha elaborado un informe de situación sobre la 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»), con el fin de informar sobre los trabajos realizados hasta la fecha por los órganos preparatorios del Consejo y sobre la situación en que se encuentra el estudio de la propuesta.

INTRODUCCIÓN

1. El 20 de enero de 2026, la Comisión propuso un nuevo paquete de ciberseguridad para reforzar la resiliencia y las capacidades de la UE en materia de ciberseguridad. El paquete consta del **Reglamento** 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 tecnologías de la información y de las comunicaciones (TIC) y por el que se deroga el Reglamento (UE) 2019/881 («Reglamento sobre la Ciberseguridad»). El presente Reglamento («Reglamento sobre la Ciberseguridad 2») se complementa con la **Directiva** por la que se modifica la Directiva (UE) 2022/2555 (Directiva SRI 2) sobre medidas de simplificación y armonización con la [Propuesta de Reglamento sobre la Ciberseguridad].

2. Antes de presentar la propuesta, el Consejo, en sus Conclusiones sobre la ENISA de 6 de diciembre de 2024[1] invitó a la Comisión a que examinara y reforzara en mayor medida la función que cumple la ENISA en apoyo a la cooperación operativa a escala de la UE y entre los Estados miembros para mejorar la ciberresiliencia, teniendo en cuenta las competencias de los Estados miembros en este ámbito. Asimismo instó a la Comisión a que velara por que el mandato de la ENISA para apoyar a los Estados miembros fuera preciso y estuviera definido claramente, con objetivos estratégicos concretos y un orden de prioridad en las tareas, además de una división más afinada entre sus tareas y competencias y las de otros agentes. El Consejo también instó a la Comisión a que aprovechara la oportunidad que constituye la evaluación del Reglamento sobre la Ciberseguridad para encontrar formas de adoptar un enfoque más sencillo, basado en el riesgo, más transparente y más rápido para el desarrollo de los esquemas europeos de certificación de la ciberseguridad. Además, en sus Conclusiones[2] de 21 de mayo de 2024 sobre el futuro de la ciberseguridad, el Consejo destacó su determinación de garantizar la seguridad de las cadenas de suministro de las TIC y puso de relieve la relevancia de los factores de riesgo no técnicos, incluida la influencia indebida de terceros Estados sobre los proveedores y prestadores. Por último, las Conclusiones del Consejo[3] de 17 de octubre de 2022 sobre la seguridad de las cadenas de suministro de las TIC subrayaron la necesidad de reforzar la resiliencia y la seguridad de las cadenas de suministro de TIC, teniendo en cuenta las repercusiones de las tensiones geopolíticas y las dependencias de los productos y servicios de TIC.

---

1 16527/24.
2 10133/24.
3 13664/22.

3. El objetivo de la propuesta de Reglamento, que se basa en el artículo 114 del TFUE, es fortalecer el marco de ciberseguridad de la Unión. Refuerza el papel y las tareas de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) para ayudar a los Estados miembros y a las entidades de la Unión a lograr un elevado nivel de ciberseguridad, resiliencia y confianza en la Unión. Su objetivo es hacer que el marco europeo de certificación de la ciberseguridad sea más eficaz y eficiente para permitir un desarrollo y una aplicación más rápidos del esquema. La propuesta también establece un marco de confianza de la Unión para la seguridad de las cadenas de suministro de TIC, que aborda los factores de riesgo no técnicos y las dependencias que afectan a la seguridad de las infraestructuras y servicios de TIC críticas. Se acompaña de medidas de simplificación específicas relacionadas con la aplicación de la Directiva SRI 2[4], destinadas a simplificar los requisitos de cumplimiento, reducir la carga administrativa innecesaria y aumentar la claridad jurídica.

4. La Hoja de Ruta «Una Europa, un mercado»[5], firmada en paralelo a la reunión informal de jefes de Estado o de Gobierno celebrada en Chipre el 24 de abril de 2026, incluye esta propuesta como uno de los resultados prioritarios.

5. El Parlamento Europeo nombró a D.ª Gregorová Markéta (Verts/ALE) ponente de la Comisión ITRE, que es la comisión competente para el fondo.

6. El 29 de abril de 2026, el Comité Económico y Social Europeo emitió un dictamen sobre la propuesta[6].

---

4 DO L 333 de 27.12.2022, p. 80.
5 8473/26.
6 8980/26.

ESTADO ACTUAL DE LOS TRABAJOS EN LOS ÓRGANOS PREPARATORIOS DEL CONSEJO

7. Se realizó una presentación general del paquete de ciberseguridad en una reunión del Grupo Horizontal «Cuestiones Cibernéticas» celebrada el 26 de enero de 2026 y en una reunión del Comité de Representantes Permanentes celebrada el 28 de enero de 2026.

8. El Grupo Horizontal «Cuestiones Cibernéticas» comenzó a debatir la propuesta el 2 de febrero de 2026, a partir de una presentación exhaustiva a cargo de la Comisión. Durante esta presentación, la Comisión también presentó las conclusiones del informe de evaluación, la ficha de financiación y la evaluación de impacto.

9. El Grupo Horizontal «Cuestiones Cibernéticas» inició la lectura de la propuesta de Reglamento el 23 de febrero de 2026.

10. Los Estados miembros acogieron favorablemente la propuesta y, en general, apoyaron sus objetivos generales, en particular el refuerzo del apoyo de la ENISA a la cooperación operativa de los Estados miembros y la optimización del marco de certificación. Sin embargo, los debates también pusieron de manifiesto que varios aspectos de la propuesta requerirían un estudio más detenido. Las delegaciones solicitaron más aclaraciones sobre el aumento de la función operativa y las tareas operativas previstas para la ENISA, como la emisión de alertas tempranas, la creación de un servicio de asistencia sobre programas de secuestro de archivos y el papel de la ENISA en la red de equipos de respuesta a incidentes de seguridad informática (CSIRT). Varias delegaciones cuestionaron las implicaciones en materia de recursos para los Estados miembros en relación con la contribución propuesta de dos expertos nacionales en comisión de servicios por Estado miembro para apoyar las tareas de la ENISA. Las normas de votación del Consejo de Administración también requieren más debates. Las delegaciones subrayaron que es necesaria mayor claridad y precisión en relación con las definiciones y conceptos utilizados en la propuesta. Asimismo es preciso aclarar más la composición del presupuesto de la ENISA, en particular el cobro de tasas.

11. En general, se acogieron positivamente las nuevas disposiciones para que el proceso de certificación sea más eficaz y eficiente, aunque se señaló la necesidad general de aumentar la participación de los Estados miembros a lo largo de todo el proceso de certificación. En términos generales, se acogió favorablemente el carácter voluntario de la certificación. Sin embargo, las delegaciones cuestionaron algunos de los plazos propuestos en el marco de certificación.

12. Los debates sobre el marco de confianza para las cadenas de suministro de TIC pusieron de relieve varias preocupaciones entre los Estados miembros. Las delegaciones pidieron más aclaraciones sobre la metodología y los procedimientos para determinar los activos de TIC clave y proveedores de alto riesgo, así como sobre el alcance y las posibles repercusiones de las medidas propuestas. Las delegaciones destacaron la importancia de garantizar un nivel adecuado de participación de los Estados miembros.

13. Varias delegaciones formularon reservas de estudio sobre distintas partes de la propuesta, en particular en relación con los aspectos de gobernanza, el uso de actos de ejecución y el mecanismo propuesto para la determinación de proveedores de alto riesgo y la seguridad de las cadenas de suministro de TIC.

14. Tras los debates en el Grupo Horizontal «Cuestiones Cibernéticas» se invitó a los Estados miembros a presentar observaciones por escrito acerca de las disposiciones relacionadas con el título I (Disposiciones generales) y el título II (ENISA). Veintitrés Estados miembros presentaron contribuciones. Posteriormente, también se invitó a los Estados miembros a presentar observaciones por escrito sobre el título III (Marco europeo de certificación de la ciberseguridad). Veinte Estados miembros aprovecharon la oportunidad para presentar por escrito su posición.

15. Sobre la base de estas contribuciones escritas de los Estados miembros y de los trabajos del Grupo Horizontal «Cuestiones Cibernéticas», la Presidencia elaborará un texto transaccional sobre los títulos II (ENISA) y III (Marco europeo de certificación de la ciberseguridad), que se presentará en la reunión del Grupo Horizontal a principios de junio de 2026.

16. Varios Estados miembros pidieron al Servicio Jurídico del Consejo que examinara la idoneidad de la base jurídica.

17. La Presidencia iniciará la lectura de las medidas de simplificación de la Directiva SRI 2 a finales de mayo de 2026.

18. En total, el Grupo Horizontal habrá celebrado durante la Presidencia chipriota quince reuniones relativas a la propuesta de Reglamento sobre la Ciberseguridad 2.

19. Tomando como base los avances logrados por la Presidencia chipriota, la Presidencia irlandesa entrante prevé proseguir los trabajos acerca de este importante expediente.

20. En vista de lo anterior, se invita al Comité de Representantes Permanentes y al Consejo a que tomen nota de los avances realizados en el examen de la propuesta de Reglamento.