Consulta pública 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 la cadena de suministro de las TIC, y por el que se deroga el Reglamento (UE) 2019/881 (Ley de Ciberseguridad 2)

Contexto

El artículo 133 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en relación con el artículo 26.2 de la Ley 50/1997, de 27 de noviembre, del Gobierno, establece que, con el objetivo de mejorar la participación de los ciudadanos en el procedimiento de elaboración de las normas, debe realizarse una consulta pública a través del portal web de la Administración competente. En ella se recabará la opinión de los sujetos y de las organizaciones más representativas potencialmente afectados por la futura norma acerca de:

- Los problemas que se pretenden solucionar con la nueva normativa.
- La necesidad y oportunidad de su aprobación.
- Los objetivos de la norma.
- Las posibles soluciones alternativas regulatorias y no regulatorias.

En cumplimiento de lo anterior, y de acuerdo con lo dispuesto en la Orden PRE/1590/2016, de 3 de octubre, por la que se publica el Acuerdo de Consejo de Ministros de 30 de septiembre de 2016, que dicta instrucciones para habilitar la participación pública en el proceso de elaboración normativa a través de los portales web de los departamentos ministeriales, se abre esta consulta pública previa.

Los ciudadanos, organizaciones y asociaciones que así lo deseen, podrán hacer llegar sus comentarios a través del FORMULARIO DE PARTICIPACIÓN adjunto.

En los comentarios que se presenten será necesario hacer constar los datos de identificación de la persona física o jurídica (nombre, apellidos, NIF) así como la denominación completa de la organización o asociación participante, en su caso. Únicamente serán tomadas en consideración las respuestas en las que la persona esté identificada.

Con carácter general, las contribuciones recibidas se considerarán susceptibles de difusión pública. Las personas físicas que no deseen la publicación de su identidad deberán manifestarlo expresamente. Asimismo, las partes de la información remitida que, a juicio de las personas interesadas, deban ser tratadas con carácter confidencial deberán ser específicamente señaladas en el propio texto de la contribución.

Objetivo de la consulta

Recoger la opinión de la ciudadanía, organizaciones y actores interesados sobre:

- Los problemas que se pretenden solucionar con la nueva norma y su adecuada identificación.
- La necesidad y oportunidad de la reforma.
- Los objetivos que debería perseguir la nueva norma.
- Las posibles alternativas regulatorias o no regulatorias.

1. Antecedentes y problemas que se pretenden solucionar con la nueva norma

La propuesta de Reglamento COM(2026) 11 final —conocida como Ley de Ciberseguridad 2 o Cybersecurity Act 2 (CSA2)— fue presentada por la Comisión Europea el 20 de enero de 2026. Su objetivo central es derogar y sustituir el Reglamento (UE) 2019/881 (Ley de Ciberseguridad) con el fin de adaptar el marco europeo de ciberseguridad a la evolución del panorama de amenazas y a los nuevos retos estratégicos y normativos.

La revisión del Reglamento vigente obedece a cuatro categorías de problemas estructurales identificados por la Comisión a partir de la evaluación del funcionamiento del marco anterior desde su entrada en vigor en 2019:

a) Desalineación entre el marco europeo de ciberseguridad y las necesidades de los actores relevantes

Desde 2019, el panorama de amenazas cibernéticas se ha intensificado de forma significativa, con un aumento de los ataques dirigidos contra infraestructuras críticas, administraciones públicas, operadores económicos y ciudadanos. Amenazas emergentes como el uso malicioso de la inteligencia artificial y la computación cuántica han transformado tanto las herramientas de defensa como las tácticas de los actores hostiles.

En este contexto, la evaluación de la Comisión concluye que las funciones y recursos de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) resultan insuficientes para responder eficazmente a las necesidades de los Estados miembros, las instituciones europeas y los actores del mercado. Concretamente, se identifican limitaciones en la capacidad de ENISA para apoyar la aplicación de las políticas de ciberseguridad de la Unión, facilitar la cooperación operativa estructurada entre los Estados miembros y dar respuesta ágil a situaciones de crisis.

b) Aplicación limitada del Marco Europeo de Certificación de la Ciberseguridad

El Reglamento (UE) 2019/881 creó el Marco Europeo de Certificación de la Ciberseguridad (ECCF, por sus siglas en inglés) como instrumento de armonización voluntaria de los esquemas nacionales de certificación de productos, servicios y procesos TIC. La evaluación posterior a su entrada en vigor constata que la aplicación práctica de este marco ha sido limitada: el proceso de elaboración y aprobación de nuevos esquemas europeos ha resultado lento y complejo, la adopción por parte del mercado ha sido insuficiente y los mecanismos de gobernanza no han permitido avanzar con la celeridad requerida.

La Comisión propone reformar el ECCF con el objetivo de ampliar su alcance —incluyendo nuevas categorías de productos, servicios, procesos TIC, y la ciberseguridad de las entidades—, agilizar los procedimientos de elaboración y mantenimiento de esquemas, y

aumentar la utilidad de los certificados europeos como herramienta de cumplimiento en el marco de distintas normas sectoriales de la Unión.

c) Fragmentación del panorama normativo de cumplimiento en ciberseguridad

El desarrollo del acervo europeo de ciberseguridad durante los últimos años —mediante la adopción de la Directiva NIS2, el Reglamento de Ciberresiliencia (CRA), el Reglamento DORA, la Directiva CER y otros instrumentos sectoriales— ha generado una pluralidad de marcos regulatorios que, aunque complementarios en sus objetivos, presentan divergencias en definiciones, procedimientos y requisitos que incrementan la complejidad del cumplimiento para las entidades obligadas.

La propuesta persigue simplificar y cohesionar el conjunto normativo de ciberseguridad, reducir la fragmentación en la aplicación de los distintos marcos e incrementar las sinergias entre los instrumentos regulatorios existentes, con especial atención a la reducción de cargas administrativas para las empresas y autoridades competentes.

En este contexto, la propuesta se articula de forma complementaria con la propuesta de Directiva de modificación de NIS2, presentada simultáneamente por la Comisión, y con la propuesta de Reglamento Ómnibus Digital, que establece para ENISA la función de punto de entrada único para la notificación de incidentes de ciberseguridad cubiertos por distintos marcos regulatorios.

d) Riesgos de ciberseguridad en las cadenas de suministro de las TIC

La creciente interdependencia de los sistemas digitales y la complejidad de las cadenas de suministro de tecnologías de la información y las comunicaciones (TIC) generan vulnerabilidades estratégicas que los enfoques nacionales fragmentados no pueden abordar con suficiente coherencia. La dependencia de determinados componentes, productos y servicios TIC respecto de proveedores o fabricantes establecidos en terceros países sujeta a la Unión a riesgos de seguridad difícilmente gestionables de forma aislada.

La propuesta introduce por primera vez un marco horizontal a nivel europeo para la gestión de los riesgos de seguridad de la cadena de suministro TIC, incluyendo tanto riesgos técnicos como no técnicos. Este marco prevé la identificación de activos TIC críticos, la posibilidad de designar proveedores de alto riesgo y la adopción de medidas proporcionadas para reducir las dependencias estratégicas, con plena observancia del principio de subsidiariedad y de la distribución de competencias entre la Unión y los Estados miembros.

2. Objetivos de la norma

Con el fin de dar respuesta a los problemas identificados en el apartado anterior, la propuesta COM(2026) 11 final persigue los siguientes objetivos:

Refuerzo del mandato de ENISA

La propuesta acomete una reforma integral del mandato de ENISA, reforzando el papel de la Agencia como principal herramienta de la Unión para la aplicación de las políticas de ciberseguridad y para el apoyo a la cooperación operativa entre los Estados miembros. Se amplían sus funciones en ámbitos como el análisis de amenazas y riesgos, la asistencia

técnica a los Estados miembros, el seguimiento del mercado de productos y servicios TIC y el apoyo a la gestión de crisis de ciberseguridad a escala europea. La propuesta prevé asimismo un incremento de los recursos financieros y humanos asignados a ENISA para que pueda ejercer eficazmente las nuevas funciones encomendadas.

Reforma y ampliación del Marco Europeo de Certificación de la Ciberseguridad

La propuesta reforma en profundidad el ECCF con el objetivo de convertirlo en un instrumento de certificación eficaz, predecible y adaptado a las necesidades del mercado y de los reguladores. Para ello, amplía el alcance del marco a nuevas categorías de objetos de certificación —incluyendo la ciberseguridad de las entidades (cyber posture)—, introduce procedimientos más ágiles para la elaboración, aprobación y mantenimiento de los esquemas europeos, revisa los mecanismos de gobernanza para garantizar una mayor participación y protagonismo de los Estados miembros en el proceso de toma de decisiones y refuerza la utilidad de los certificados como herramienta de cumplimiento en el marco del acervo europeo de ciberseguridad.

Simplificación y coherencia del marco normativo

La propuesta persigue una mayor coherencia e interoperabilidad entre los distintos instrumentos del acervo europeo de ciberseguridad, en particular en materia de requisitos, definiciones y procedimientos. En este sentido, prevé modificaciones orientadas a la simplificación del cumplimiento normativo para las entidades sujetas a múltiples marcos regulatorios y a la reducción de las cargas administrativas tanto para los operadores económicos como para las autoridades competentes de los Estados miembros.

Adicionalmente, en el ámbito de la notificación de incidentes, la propuesta se articula con las reformas previstas en el Ómnibus Digital, que crea un mecanismo centralizado de notificación gestionado por ENISA para que las entidades puedan cumplir simultáneamente con sus obligaciones de notificación derivadas de distintos marcos regulatorios.

Marco europeo de seguridad de la cadena de suministro TIC

La propuesta establece un marco armonizado a nivel europeo para la identificación y gestión de los riesgos de ciberseguridad en las cadenas de suministro de las TIC. Este marco introduce un mecanismo de identificación de activos TIC críticos, define los criterios para la posible designación de proveedores de alto riesgo —considerando tanto factores técnicos como no técnicos— y habilita la adopción de medidas proporcionadas de restricción, condicionamiento o exclusión en ámbitos críticos.

El diseño de este marco contempla la participación activa de los Estados miembros en los procedimientos de evaluación de riesgos y en la adopción de las medidas correspondientes, así como la necesaria articulación con los marcos nacionales existentes, los períodos de transición adecuados y la evaluación rigurosa del impacto económico, operativo y diplomático de las medidas que pudieran adoptarse.