LEY DE CIBERRESILIENCIA EUROPEA

Reglamento (UE) 2024/2847 — Tutorial para Responsables de TI, Cumplimiento y Desarrollo de Producto

Actualizado a mayo de 2026

Introducción

La Ley de Ciberresiliencia europea —aprobada formalmente como Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo— constituye el primer marco normativo horizontal de la Unión Europea específicamente dirigido a garantizar la seguridad de los productos con elementos digitales durante todo su ciclo de vida. La norma responde a un contexto de creciente digitalización en el que millones de dispositivos conectados, aplicaciones de software y servicios en línea son desplegados en el mercado interior sin requisitos mínimos armonizados de ciberseguridad.

El presente documento tiene por objeto proporcionar a directores de Tecnología de la Información, responsables de cumplimiento normativo y equipos de desarrollo de producto una guía estructurada y práctica sobre el contenido, el alcance, las obligaciones y el calendario de aplicación de esta norma. Las referencias utilizadas proceden de fuentes oficiales de la Unión Europea, en particular del texto publicado en el Diario Oficial de la UE y de la documentación técnica de la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

Sección 1: Definición y Alcance

La Ley de Ciberresiliencia define como «producto con elementos digitales» cualquier producto de software o hardware, así como sus soluciones de procesamiento remoto de datos, que incluya funciones de procesamiento de datos conectadas directa o indirectamente a una red. La norma fija como objetivo principal garantizar que los productos se diseñen, desarrollen y mantengan con un nivel adecuado de ciberseguridad desde su concepción hasta el final de su vida útil —principio conocido como security by design—, y que los operadores económicos adopten las medidas necesarias para gestionar las vulnerabilidades que surjan con posterioridad a la comercialización.

Conforme al artículo 2 del Reglamento, el ámbito de aplicación es de carácter horizontal: abarca a fabricantes, importadores y distribuidores establecidos o que comercializan productos en el mercado único europeo, con independencia del sector o la tecnología empleada. Se excluyen expresamente del ámbito de aplicación los productos ya sujetos a regulación sectorial equivalente, como los dispositivos sanitarios regulados por el Reglamento (UE) 2017/745 o los equipos de aviación cubiertos por el Reglamento (UE) 2018/1139.

Los objetivos estratégicos del Reglamento pueden resumirse en tres ejes principales:

- Elevar el nivel de ciberseguridad de los productos digitales que circulan en el mercado interior europeo, reduciendo la superficie de ataque a escala sistémica.
- Asegurar la transparencia sobre las propiedades de seguridad, obligando a los fabricantes a proporcionar información clara y accesible a los usuarios finales.

- Atribuir responsabilidades claras a los operadores económicos a lo largo de toda la cadena de valor, desde el diseño hasta la gestión post-comercialización de vulnerabilidades.

A título ilustrativo: una empresa fabricante de routers domésticos con sede en Alemania que vende sus productos en toda la Unión Europea queda sujeta íntegramente a la norma. Del mismo modo, un desarrollador de software de gestión empresarial (ERP) que incorpore módulos de conectividad a red debe cumplir los requisitos esenciales de ciberseguridad del Anexo I del Reglamento antes de colocar su producto en el mercado.

Referencia normativa clave

Artículo 2, Artículo 3 (definiciones) y Considerando 12 del Reglamento (UE) 2024/2847. Publicado en el Diario Oficial de la Unión Europea, serie L, el 20 de noviembre de 2024.

Sección 2: Implicaciones para las Empresas

2.1 Requisitos esenciales de ciberseguridad

El Anexo I del Reglamento establece los requisitos esenciales aplicables a todo producto con elementos digitales. Estos se estructuran en dos categorías: requisitos relativos a las propiedades del producto y requisitos de gestión de vulnerabilidades. Entre los primeros destacan:

- Diseño y desarrollo con superficie de ataque mínima, incluyendo interfaces de red y protocolos de comunicación.
- Mecanismos de autenticación y control de acceso proporcionales al nivel de riesgo del producto.
- Protección de la confidencialidad e integridad de los datos, tanto en reposo como en tránsito.
- Capacidad de actualización de seguridad —patches— durante un período mínimo de cinco años desde la comercialización, o durante el ciclo de vida esperado si este fuese inferior.
- Generación de registros de auditoría (logs) y notificación automática de incidentes cuando resulte aplicable.

2.2 Proceso de evaluación de la conformidad y marcado CE

De conformidad con el artículo 27 del Reglamento, todos los productos con elementos digitales deben someterse a un proceso de evaluación de la conformidad antes de ser comercializados y ostentar el marcado CE. El procedimiento varía según la clasificación del producto:

- Productos estándar (Clase I): el fabricante puede efectuar una autoevaluación (módulo A) siempre que aplique normas armonizadas o especificaciones técnicas comunes.
- Productos importantes (Clase II) y críticos (Clase III): se requiere la intervención de un organismo notificado (third-party conformity assessment body) para la revisión del módulo de aseguramiento de la calidad o el examen de tipo UE.

Ejemplo aplicado: un fabricante de cámaras de seguridad IP clasificadas como Clase II deberá contratar a un organismo notificado acreditado —conforme al Reglamento (CE) n.º 765/2008— para obtener la certificación antes de su comercialización en el mercado único.

2.3 Obligaciones de reporte de vulnerabilidades e incidentes

El artículo 14 del Reglamento introduce un sistema de notificación escalonado obligatorio. Los fabricantes deben:

- Notificar sin dilación indebida —y en todo caso en un plazo máximo de 24 horas— a ENISA y a la autoridad de supervisión nacional cualquier vulnerabilidad activamente explotada de la que tengan conocimiento.
- Presentar, en el plazo de 72 horas, una notificación inicial con los primeros análisis del impacto y las medidas de mitigación adoptadas.
- Remitir, en el plazo de 14 días desde el conocimiento del incidente, un informe final que incluya una descripción detallada, el nivel de gravedad y las correcciones implementadas.

Este sistema de reporte se integra con el marco establecido por la Directiva (UE) 2022/2555 (NIS2), evitando duplicidades para los operadores que sean simultáneamente sujetos de ambas normas.

Ejemplo de cumplimiento avanzado

Cisco Systems ha publicado un roadmap público de adecuación a la Ley de Ciberresiliencia, incorporando en su ciclo seguro de desarrollo de software (SDL) los controles del Anexo I y los flujos de notificación del artículo 14. Por su parte, la empresa española Telefónica ha integrado los requisitos de la norma en su programa de certificación de proveedores industriales. Fuente: comunicaciones corporativas de ambas compañías, primer trimestre de 2026.

Sección 3: Productos y Sectores Afectados

El Reglamento establece una clasificación tripartita de los productos con elementos digitales, atendiendo a su criticidad para la ciberseguridad del mercado interior. Esta categorización determina el nivel de exigencia en la evaluación de la conformidad:

3.1 Productos estándar

Constituyen la mayoría de los productos digitales del mercado, siempre que no se encuadren en las categorías de mayor riesgo. Son ejemplos representativos:

- Dispositivos de domótica inteligente de consumo (altavoces inteligentes, termostatos conectados, bombillas IoT).
- Aplicaciones de software de productividad ofimática con conectividad a red.
- Wearables de uso general no dirigidos a infraestructuras críticas.

3.2 Productos importantes (Clase I y Clase II)

El Anexo III del Reglamento enumera los productos considerados importantes, clasificados a su vez en Clase I —sometidos a autoevaluación asistida— y Clase II —que requieren intervención de organismo notificado—. Entre los ejemplos relevantes se incluyen:

- Clase I: sistemas operativos para uso general, navegadores web, gestores de contraseñas, antivirus y software de seguridad endpoint.
- Clase II: hipervisores y sistemas de gestión de contenedores (container management), sistemas de detección y respuesta ante intrusiones (IDS/IPS), microprocesadores de uso general, tarjetas inteligentes y elementos seguros.

Un fabricante de soluciones SIEM (Security Information and Event Management) quedaría encuadrado en la Clase II, dado que este tipo de producto constituye un componente de seguridad crítico para la protección de infraestructuras de red.

3.3 Productos críticos

El Anexo IV identifica los productos de mayor criticidad para la infraestructura digital europea. Actualmente comprende:

- Hardware con funciones de seguridad integradas: tarjetas criptográficas, módulos de plataforma de confianza (TPM), enclaves seguros.
- Equipos de red de uso crítico: routers y módems para uso empresarial e industrial, así como switches de capa de distribución en redes de operadores.

3.4 Sectores con mayor impacto

Los sectores que experimentarán un impacto regulatorio más significativo son: fabricación de dispositivos IoT industriales y de consumo, industria del software (SaaS, plataformas embebidas), telecomunicaciones y operadores de red, sistemas de automatización industrial y SCADA, sector sanitario con dispositivos conectados no médicos, y automoción en lo relativo a sistemas de info-entretenimiento y conectividad vehicular.

Ejemplo sectorial ilustrativo: una empresa fabricante de equipos de control industrial (PLCs) para plantas de tratamiento de agua deberá obtener la evaluación de un organismo notificado y mantener un programa activo de gestión de vulnerabilidades conforme a los artículos 13 y 14 del Reglamento, dado que sus productos presentan potencial impacto en infraestructuras críticas.

Fuente oficial de referencia para clasificación de productos

Anexos III y IV del Reglamento (UE) 2024/2847. ENISA mantiene actualizada una guía de clasificación de productos disponible en: https://www.enisa.europa.eu/topics/cyber-resilience-act

Sección 4: Calendario de Implementación

El Reglamento (UE) 2024/2847 fue publicado en el Diario Oficial de la Unión Europea el 20 de noviembre de 2024 y entró en vigor el 10 de diciembre de 2024. No obstante, su plena aplicabilidad se despliega de manera escalonada:

- 10 de diciembre de 2024: entrada en vigor del Reglamento. Inicio del período de adaptación para los operadores económicos.
- 11 de septiembre de 2026: fecha de aplicación de las obligaciones de supervisión del mercado y notificación de incidentes establecidas en el artículo 14 (adelantada respecto al plazo general para garantizar coordinación con NIS2).
- 11 de diciembre de 2027: fecha de plena aplicabilidad del Reglamento. A partir de esta fecha, ningún producto con elementos digitales que no cumpla los requisitos esenciales del Anexo I podrá ser comercializado en el mercado único europeo.

Los fabricantes que hayan comercializado productos antes del 11 de diciembre de 2027 disponen de un régimen transitorio: podrán continuar comercializando existencias ya producidas, pero los nuevos lotes deberán cumplir íntegramente la norma. Asimismo, el período comprendido entre 2024 y 2027 está siendo utilizado por la Comisión Europea para desarrollar normas armonizadas —mediante mandato al CEN/CENELEC— que faciliten la evaluación de la conformidad técnica.

Recomendación: Las empresas deben iniciar su proceso de adecuación con al menos 18 meses de antelación a la fecha límite, dado que los procesos de evaluación de conformidad con organismos notificados pueden requerir entre 6 y 12 meses según la complejidad del producto.

Fechas clave resumidas

10 dic. 2024: Entrada en vigor. — 11 sep. 2026: Obligaciones de reporte activas. — 11 dic. 2027: Plena aplicabilidad y prohibición de comercialización de productos no conformes. Fuente: artículo 71 del Reglamento (UE) 2024/2847.

Sección 5: Consejos Prácticos para la Adaptación

5.1 Evaluación inicial de la cartera de productos

El primer paso consiste en elaborar un inventario completo de los productos con elementos digitales que la organización fabrica, importa o distribuye, y clasificarlos conforme a los Anexos III y IV del Reglamento. Para ello se recomienda constituir un equipo multidisciplinar integrado por responsables de TI, ingeniería de producto, legal y cumplimiento. ENISA ha publicado una guía metodológica de análisis de impacto disponible en su portal oficial.

5.2 Integración de security by design en el ciclo de desarrollo

Las organizaciones deben revisar y, en su caso, reforzar sus procesos de desarrollo de software y hardware para incorporar los requisitos del Anexo I desde las fases tempranas de diseño. Se recomiendan las siguientes medidas:

- Adopción de un Ciclo de Vida de Desarrollo Seguro (SDL) documentado, alineado con estándares reconocidos como IEC 62443-4-1 o ISO/IEC 27034.
- Implementación de herramientas de análisis de composición de software (SCA) para la gestión de dependencias de terceros y la detección temprana de vulnerabilidades en componentes de código abierto.
- Realización de pruebas de penetración periódicas y auditorías de código previas al lanzamiento de cada versión del producto.
- Establecimiento de un proceso formal de gestión de vulnerabilidades post-comercialización, incluyendo canales públicos de divulgación responsable (Coordinated Vulnerability Disclosure, CVD) conforme al artículo 13 del Reglamento.

5.3 Preparación documental y gestión de la conformidad

El Reglamento exige a los fabricantes mantener una declaración de conformidad UE y conservar la documentación técnica durante un período mínimo de diez años tras la comercialización del producto (artículo 31). Se recomienda:

- Designar un responsable de cumplimiento normativo en materia de ciberseguridad de producto (Product Security Officer) con reporte directo a la dirección.
- Implementar un sistema de gestión documental que centralice los expedientes técnicos, certificados de conformidad y registros de notificaciones a autoridades.
- Establecer procedimientos internos de respuesta ante vulnerabilidades que incluyan plantillas de notificación compatibles con los requisitos del artículo 14 y los plazos de 24, 72 horas y 14 días.

5.4 Gestión de la cadena de suministro

La responsabilidad del fabricante no se limita a los componentes propios: el artículo 13 establece la obligación de gestionar los riesgos de ciberseguridad derivados de componentes de terceros integrados en el producto final. Ello implica incorporar cláusulas de ciberseguridad en los contratos con proveedores y exigir la provisión de un Software Bill of Materials (SBOM) para los componentes críticos.

Ejemplo de buena práctica

La empresa Bosch, fabricante de componentes IoT industriales, ha implementado un programa interno denominado 'Product Security Incident Response Team' (PSIRT) conforme a los requisitos de la norma, incluyendo plazos de notificación alineados con el artículo 14 y un portal público de divulgación de vulnerabilidades. Esta iniciativa es citada por ENISA como referencia de buena práctica en su informe 'Good Practices for Security of IoT' (actualización 2025).

Conclusión

La Ley de Ciberresiliencia europea supone un cambio estructural en la forma en que fabricantes, desarrolladores e importadores conciben y gestionan la seguridad de sus productos digitales. Lejos de constituir una carga meramente burocrática, la norma ofrece a las organizaciones conformes una ventaja competitiva significativa en un mercado interior en el que la confianza de los consumidores e industrias en la seguridad de los productos digitales es un factor diferenciador creciente.

El cumplimiento efectivo requiere una aproximación proactiva, transversal y sostenida en el tiempo: no se trata de un ejercicio puntual de certificación, sino de la incorporación permanente de la ciberseguridad en los procesos de innovación y comercialización. Las organizaciones que inicien su proceso de adecuación con anticipación estarán mejor posicionadas para afrontar los plazos regulatorios de 2026 y 2027 sin disrupciones en su actividad comercial.

Para profundizar en los aspectos técnicos y normativos, se recomienda consultar el texto íntegro del Reglamento (UE) 2024/2847 en el portal EUR-Lex (eur-lex.europa.eu) y los recursos actualizados de ENISA (enisa.europa.eu), que incluyen guías sectoriales, herramientas de autoevaluación y documentación de estándares armonizados en desarrollo.

— Fin del documento —