WHITEPAPER DE CRA EVIDENCE

La Ley de Ciberresiliencia de la UE: guía práctica de cumplimiento

Libro blanco para fabricantes, importadores y distribuidores de productos con elementos digitales.

Preparado por	CRA Evidence
Versión	1.0
Estado	Documento vivo
Base	Regulation (EU) 2024/2847

Historial de cambios

Esta guía se actualiza a medida que evolucionan las orientaciones de la Comisión, las normas armonizadas y la práctica de mercado bajo el CRA.

Versión	Fecha	Descripción
1.0	17 de mayo de 2026	Publicación pública inicial. Cubre ámbito, clasificación, modificación sustancial, requisitos esenciales, gestión de vulnerabilidades, expediente técnico, vías de conformidad e interacción con AI Act, Data Act, ESPR y responsabilidad por producto.

Índice

Resumen ejecutivo

EN 60 SEGUNDOS

Ámbito: hardware conectado y productos de software introducidos en el mercado de la UE, con la seguridad tratada como requisito de cumplimiento de producto y no como buena práctica.

Fechas clave: notificaciones del artículo 14 desde el 11 de septiembre de 2026; obligaciones técnicas, documentales y de marcado CE completas desde el 11 de diciembre de 2027.

Entregables: evaluación de riesgos de ciberseguridad, SBOM, expediente técnico, instrucciones de usuario, declaración UE de conformidad, marcado CE y notificaciones de incidentes y vulnerabilidades del artículo 14.

Quién debe actuar

Los fabricantes asumen la carga principal. Importadores y distribuidores tienen comprobaciones de diligencia antes de poner productos a disposición.

Qué cambia

La ciberseguridad pasa a ser cumplimiento de producto: diseño seguro, gestión de vulnerabilidades, documentación, marcado CE y actuación posterior a la comercialización.

Primer plazo

Las notificaciones del artículo 14 empiezan el **11 de septiembre de 2026** para vulnerabilidades explotadas activamente e incidentes graves.

Aplicación completa

El cumplimiento técnico completo se aplica desde el **11 de diciembre de 2027**. Los productos anteriores quedan cubiertos tras una modificación sustancial, pero la notificación sigue aplicando.

Columna vertebral de evidencia

El expediente técnico necesita la evaluación de riesgos, SBOM, justificación del soporte, evidencia de ensayos, instrucciones de usuario, declaración y prueba de conformidad con los requisitos esenciales de ciberseguridad.

Vía de conformidad

La mayoría de productos puede usar el módulo A. Los productos importantes y críticos pueden requerir organismo notificado o certificación europea de ciberseguridad.

Qué es la Ley de Ciberresiliencia

La Ley de Ciberresiliencia es el nombre público usado en España para Regulation (EU) 2024/2847, cuyo título formal en español es Reglamento de Ciberresiliencia. Es el primer marco de la UE que convierte la ciberseguridad en un requisito vinculante para productos con elementos digitales introducidos en el mercado de la UE. El texto oficial está disponible en EUR-Lex.

La Ley de Ciberresiliencia se aplica a fabricantes, importadores y distribuidores de hardware y software conectados. Cubre desde dispositivos IoT de consumo hasta sistemas de control industrial. El cambio práctico es claro: la ciberseguridad ahora debe diseñarse, evidenciarse, mantenerse y monitorizarse como parte del cumplimiento del producto.

El incumplimiento de los requisitos esenciales de ciberseguridad o de las obligaciones de los artículos 13 y 14 puede acarrear sanciones de hasta 15 millones de euros o el 2,5% del volumen de negocios anual mundial, según cuál sea mayor. Se aplican tramos inferiores: hasta 10 millones de euros o el 2% por incumplir otras obligaciones especificadas, y hasta 5 millones de euros o el 1% por facilitar información incorrecta, incompleta o engañosa a los organismos notificados o a las autoridades de vigilancia del mercado. Las autoridades de vigilancia del mercado también pueden exigir acciones correctivas, restringir la disponibilidad, retirar productos del mercado o exigir recuperaciones.

Fechas clave para planificar el cumplimiento

La Ley de Ciberresiliencia entró en vigor el **10 de diciembre de 2024**. El trabajo práctico de cumplimiento se organiza en tres hitos: organismos notificados en **junio de 2026**, notificación en **septiembre de 2026** y cumplimiento técnico completo en **diciembre de 2027**.

NOTA

Estado de las orientaciones de la Comisión: La Comisión Europea publicó el borrador de orientaciones sobre el CRA el 3 de marzo de 2026. La consulta se cerró el 13 de abril de 2026. Las orientaciones no son definitivas, pero son útiles para planificar la introducción en el mercado, el software libre y de código abierto, los periodos de soporte, las modificaciones sustanciales, la clasificación de productos, la diligencia debida sobre componentes, el tratamiento remoto de datos, la gestión de vulnerabilidades y los solapamientos con otros textos de la UE. Algunas cuestiones de frontera, incluidas las relativas al AI Act y DORA, pueden requerir más orientación.

10 de diciembre de 2024

Entrada en vigor

Empieza el periodo transitorio

11 de junio de 2026

Organismos notificados

Se aplica el capítulo IV

11 de septiembre de 2026

Notificación

Empiezan las notificaciones del artículo 14

11 de diciembre de 2027

Aplicación completa

Requisitos técnicos, marcado CE, documentación y evaluación de la conformidad

HAZ ESTO PRIMERO

Empieza por la preparación para notificar. El plazo del artículo 14 llega antes que el cumplimiento técnico completo y se aplica a productos que ya están en el mercado de la UE.

Como la notificación empieza el **11 de septiembre de 2026**, la preparación para notificar debe ser el primer frente de trabajo: **detección, triaje, notificación a usuarios y notificación a autoridades** deben funcionar antes de que venza el cumplimiento técnico completo.

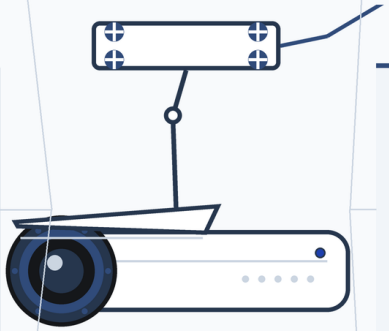
Los productos con elementos digitales introducidos en el mercado antes del **11 de diciembre de 2027** solo quedan sujetos a los requisitos técnicos de la Ley de Ciberresiliencia si sufren una **modificación sustancial** desde esa fecha. Las notificaciones del artículo 14 son distintas: se aplican a **todos los productos dentro del ámbito**, incluidos los introducidos en el mercado antes de esa fecha.

La Ley de Ciberresiliencia en el ciclo de vida del producto

PASO 01
Definir el alcance
Ámbito, clasificación, periodo de soporte y evaluación de riesgos

PASO 02
Desarrollar de forma segura
Valores seguros por defecto, análisis de código, SBOM y control de dependencias

PASO 03
Validar y documentar
Pruebas, triaje de vulnerabilidades, expediente técnico e instrucciones



PASO 04
Lanzar al mercado
Declaración UE de conformidad, marcado CE y decisión de lanzamiento

PASO 05
Vigilar y actualizar
CVE, avisos, actividad de explotación, actualizaciones y divulgación

PASO 06
Dar soporte y cooperar
Artículo 14, avisos a usuarios, solicitudes de autoridades y fin de soporte

Cámara IP conectada, de la planificación al soporte poscomercialización bajo la Ley de Ciberresiliencia

Qué productos entran en el ámbito de aplicación

Ámbito y exclusiones

La Ley de Ciberresiliencia se aplica a productos de hardware y software cuyo uso previsto o razonablemente previsible incluya una conexión de datos directa o indirecta con un dispositivo o red. Esto incluye ordenadores, smartphones, equipos de red, dispositivos IoT, sistemas de control industrial y aplicaciones de tratamiento de datos.

Estas categorías quedan excluidas de forma expresa:

- Productos sanitarios y productos sanitarios para diagnóstico in vitro cubiertos por los Reglamentos (UE) 2017/745 y 2017/746
- Sistemas de automoción cubiertos por el Reglamento (UE) 2019/2144
- Equipos aeronáuticos cubiertos por el Reglamento (UE) 2018/1139
- Equipos marinos cubiertos por la Directiva 2014/90/UE
- Productos desarrollados exclusivamente con fines de seguridad nacional o defensa
- Productos puramente mecánicos sin elementos digitales ni conectividad de red

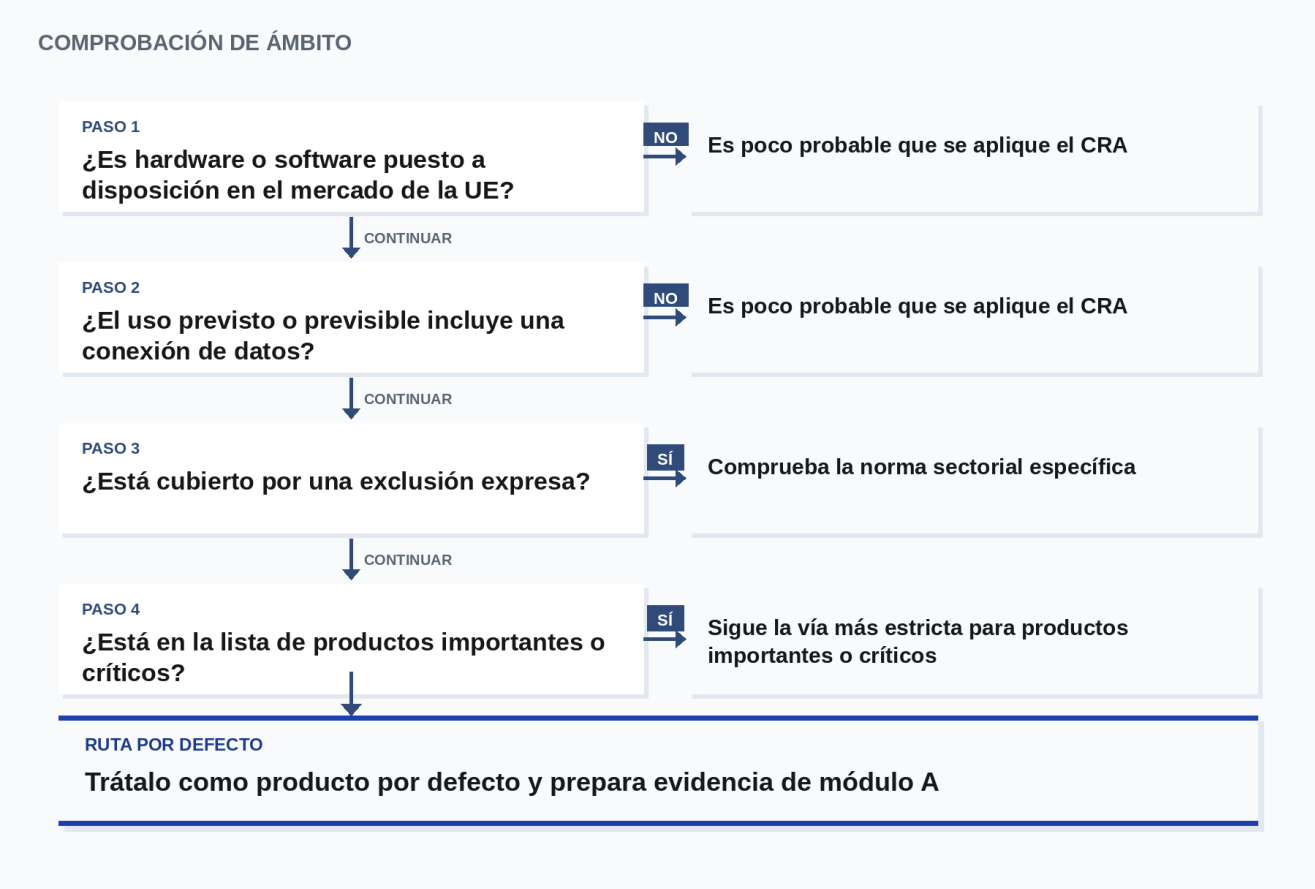
Si no hay una exclusión clara, asume que tu producto conectado entra en el ámbito.

NOTA

Productos a medida: una excepción estrecha. Si construyes un producto ajustado a un usuario empresarial concreto, bajo un acuerdo escrito entre tu empresa y ese usuario, puedes apartarte de dos requisitos solamente: la configuración segura por defecto, manteniendo siempre una vía de retorno a un estado original seguro, y las actualizaciones de seguridad gratuitas, cuya base comercial puede fijarse en el acuerdo. Todo lo demás se aplica íntegramente: gestión de vulnerabilidades, el resto de requisitos de seguridad del producto, notificaciones del artículo 14, documentación técnica, marcado CE, evaluación de la conformidad y periodo de soporte. No es una excepción B2B general y no cubre los productos estándar vendidos a empresas.

RESPONSABILIDADES DE LOS OPERADORES ECONÓMICOS

Fabricante	Diseñar productos seguros, evaluar riesgos, preparar documentación técnica, ejecutar la evaluación de la conformidad, gestionar vulnerabilidades y notificar eventos del artículo 14.
Importador	Comprobar el cumplimiento del fabricante, verificar el marcado CE y la documentación, mantener disponible la declaración y actuar ante vulnerabilidades conocidas.
Distribuidor	Comprobar indicadores de diligencia antes del suministro, verificar la información y las instrucciones obligatorias, y evitar poner a disposición productos no conformes.



La clasificación del producto determina la vía de evaluación

La categoría de tu producto determina cómo demuestras la conformidad.

Categoría	Ejemplos	Evaluación de la conformidad
Por defecto "no clasificado"	Software general y productos de consumo conectados que no figuran en las categorías Importante o Crítico	Módulo A: autoevaluación
Importante "Clase I"	Identidad, navegador, gestor de contraseñas, antivirus, VPN, gestión de red, router, cerradura inteligente, cámara de seguridad y productos similares	Módulo A solo cuando se apliquen las normas armonizadas, especificaciones comunes o esquemas de certificación aplicables según lo exigido; en caso contrario, módulo B+C o módulo H
Importante "Clase II"	Hipervisores, entornos de ejecución de contenedores, cortafuegos, IDS/IPS y microprocesadores resistentes a manipulaciones	Módulo B+C, módulo H o un esquema europeo de certificación de ciberseguridad aplicable con nivel de garantía al menos "sustancial"
Productos críticos	Elementos seguros, tarjetas inteligentes, pasarelas de contadores inteligentes y cajas de seguridad por hardware	Certificación europea de ciberseguridad cuando sea exigida y esté disponible; en caso contrario, se aplican las vías de Clase II

Las cuatro categorías de producto

La tabla anterior recoge ejemplos. La referencia completa, frente a la que comparas la funcionalidad principal de tu producto, aparece a continuación.

Productos por defecto

La mayoría de productos acaba aquí. Cualquier producto con elementos digitales cuya funcionalidad principal no figure en las listas de Importante o Crítico se trata como Por defecto. La vía de conformidad es la autoevaluación bajo módulo A.

Ejemplos habituales:

- Smart TVs y dispositivos de streaming.
- Impresoras de red y dispositivos multifunción de oficina.
- Altavoces Bluetooth y productos de audio de consumo.
- Aplicaciones de reproductor multimedia.
- Consolas, lectores de libros electrónicos y similares electrónicos de consumo.
- Pequeños electrodomésticos inteligentes como hornos, frigoríficos y lavavajillas sin funciones de seguridad.
- Bombillas inteligentes e iluminación conectada sin funciones de seguridad.
- Pulseras de actividad sin finalidad de monitorización sanitaria.
- Aplicaciones móviles de propósito general que no son navegadores, gestores de contraseñas ni VPN.
- Ofimática como procesadores de texto y hojas de cálculo.

La lista anterior es ilustrativa. Las listas de Importante y Crítico que siguen son exhaustivas.

Productos importantes (Clase I)

Evaluación obligatoria por tercero, salvo que se apliquen normas armonizadas, especificaciones comunes o esquemas de certificación aplicables según lo exigido.

1. Software y hardware de gestión de identidades y de accesos privilegiados, incluidos lectores de autenticación y control de acceso (lectores biométricos incluidos).
2. Navegadores autónomos e integrados.
3. Gestores de contraseñas.
4. Software que busca, elimina o pone en cuarentena software malicioso.
5. Productos VPN.
6. Sistemas de gestión de redes.
7. Sistemas de gestión de información y eventos de seguridad (SIEM).
8. Gestores de arranque.
9. Software de infraestructura de clave pública y emisión de certificados digitales.
10. Interfaces de red físicas y virtuales.
11. Sistemas operativos.
12. Routers, módems destinados a conectarse a internet y switches.
13. Microprocesadores con funcionalidades relacionadas con la seguridad.
14. Microcontroladores con funcionalidades relacionadas con la seguridad.
15. ASIC y FPGA con funcionalidades relacionadas con la seguridad.
16. Asistentes virtuales de propósito general para el hogar inteligente.

17. Productos de hogar inteligente con funcionalidades de seguridad (cerraduras inteligentes, cámaras de seguridad, monitores para bebés, sistemas de alarma).
18. Juguetes conectados a internet con funciones interactivas (habla, grabación, seguimiento de ubicación).
19. Dispositivos vestibles personales con finalidad de monitorización sanitaria (cuando no se apliquen los Reglamentos (UE) 2017/745 o 2017/746), o vestibles destinados a niños.

Productos importantes (Clase II)

Evaluación obligatoria por tercero, vía más estricta. La autoevaluación no está disponible aunque existan normas armonizadas.

1. Hipervisores y entornos de ejecución de contenedores que admiten la ejecución virtualizada de sistemas operativos y entornos similares.
2. Cortafuegos, sistemas de detección y prevención de intrusiones.
3. Microprocesadores resistentes a manipulaciones.
4. Microcontroladores resistentes a manipulaciones.

Productos críticos

Certificación europea de ciberseguridad cuando el esquema esté disponible. En caso contrario, se aplica la vía de Clase II.

1. Dispositivos de hardware con cajas de seguridad.
2. Pasarelas de contadores inteligentes dentro de los sistemas de medición inteligente, según se definen en el artículo 2, punto 23, de la Directiva (UE) 2019/944, y otros dispositivos con fines de seguridad avanzada, incluido el procesamiento criptográfico seguro.
3. Tarjetas inteligentes y dispositivos similares, incluidos elementos seguros.

Si la funcionalidad principal de tu producto coincide con una entrada de la lista de Importante o Crítico, tu producto cae en esa clase. Si tu producto integra una de esas entradas como componente pero su propia funcionalidad principal es otra cosa, la integración no cambia tu clase.

Cómo clasificar: funcionalidad principal, no integración

Las listas anteriores te dicen cuáles son las categorías. No te dicen cómo aplicarlas a tu producto. La respuesta del CRA es un único término: **funcionalidad principal**.

Tu clase la determina cuál es la funcionalidad principal de tu producto, no qué componentes integra. Si esa funcionalidad coincide con la lista de Importante, el producto es Importante (Clase I o Clase II). Si coincide con la lista de Crítico, el producto es Crítico. Si no coincide con ninguna, el producto es Por defecto. Esa es toda la prueba.

La salvaguarda práctica está en la segunda frase del artículo 7(1). Integrar un componente Importante no convierte al producto integrador en Importante. Embeber una biblioteca de cortafuegos en un hub de hogar inteligente no convierte al hub en cortafuegos. El considerando 45 lo dice con claridad: los cortafuegos y los sistemas de detección de intrusiones son Clase II Importante, pero los demás productos que los integran no lo son.

Usa esta secuencia para autoclasificarte.

1. **Enuncia la funcionalidad principal de tu producto en una frase.** Si no puedes, el resto del análisis falla. Céntrate en aquello sin lo que el producto no funcionaría.
2. **Comprueba la lista de Importante.** Una coincidencia en Clase I o II convierte al producto en Importante.
3. **Comprueba la lista de Crítico.** Una coincidencia convierte al producto en Crítico. Se aplica la vía de certificación europea de ciberseguridad cuando el esquema esté disponible; en caso contrario, la vía de Clase II.
4. **Sin coincidencia en ninguna lista.** El producto es Por defecto. La vía es la autoevaluación bajo módulo A.
5. **Documenta el razonamiento.** Un memorándum de una página con el enunciado de funcionalidad principal, la comprobación frente a las listas y la vía elegida pertenece al expediente técnico.

Dos ejemplos resueltos.

Hub de hogar inteligente con gestor de contraseñas embebido. Funcionalidad principal: orquestar rutinas entre dispositivos IoT de consumo en un hogar. El componente gestor de contraseñas, vendido por separado por su propio fabricante, es por sí solo un producto Importante Clase I. La funcionalidad principal del hub es la automatización del hogar, no la gestión de credenciales. El hub sigue siendo Por defecto.

Sistema operativo por conjunto de funciones. Un producto se comercializa como electrodoméstico inteligente, pero sus funciones principales son la inicialización de hardware y periféricos, la planificación de procesos, la gestión de memoria y una interfaz de llamadas al sistema. Esa es la funcionalidad principal de un sistema operativo. Los sistemas operativos son productos Importante Clase I. El producto es Importante Clase I, al margen del envoltorio de marketing.

Si tu clasificación cae en una clase que sorprende al resto del equipo, el enunciado de funcionalidad principal necesita otra pasada antes de lanzar.

Cuando la nube forma parte de tu producto

La mayoría de productos con elementos digitales se apoyan en algo fuera del dispositivo: un backend en la nube, una app móvil acompañante, un servidor de actualizaciones por aire, un portal de autenticación, un sistema de gestión de dispositivos. El CRA no trata todo eso como tu producto. Lo trata como parte del producto solo cuando se cumplen **dos** condiciones:

- El software ha sido **diseñado y desarrollado por tu equipo, o bajo tu responsabilidad**.
- El producto **no podría realizar una de sus funciones** sin él.

Si alguna condición falla, el servicio remoto queda fuera del perímetro del producto a efectos del CRA. Un SaaS de un tercero que tú no controlas, aunque tu producto hable con él, no forma parte de tu producto. Una web que promociona el producto pero no soporta sus funciones tampoco forma parte de tu producto.

Cuando un componente remoto entra en el ámbito, entra **como parte del producto**. El expediente técnico, la evaluación de la conformidad, la declaración de conformidad, la gestión de vulnerabilidades y los plazos de notificación del artículo 14 cubren el componente en la nube junto con el dispositivo.

Usa esta matriz para resolver el caso rápido.

Componente	¿Dentro del ámbito como parte del producto?
App móvil acompañante que se empareja con el dispositivo	**Sí.** La diseñas tú y el dispositivo no se configura ni se usa sin ella.
Backend en la nube que almacena y procesa los datos del dispositivo	**Sí.** Lo diseñas tú y el panel o la función principal no funciona sin él.
Servidor de actualizaciones por aire	**Sí.** Lo diseñas tú y el dispositivo no puede recibir actualizaciones de seguridad sin él.
Portal de autenticación que controla el acceso al dispositivo	**Sí.** Lo diseñas tú y los usuarios no pueden iniciar sesión sin él.
Sitio web de marketing del producto	**No.** No soporta una función del producto.
SaaS de tercero con el que el producto se integra (no es tuyo)	**No.** No diseñado por ti. El proveedor tercero tiene sus propias obligaciones bajo NIS 2.
Infraestructura genérica en la nube donde corre tu servicio (IaaS o PaaS)	**No.** No diseñada por ti. El proveedor de infraestructura cae bajo NIS 2.

Un patrón frecuente: un dispositivo de hogar inteligente con app móvil, servidor de actualizaciones y backend en la nube. Los tres los diseña el fabricante y el dispositivo no puede realizar sus funciones anunciadas sin ellos. Los tres forman parte del producto. Las obligaciones del CRA se aplican al conjunto. Si después el backend en la nube habla con un SaaS de analítica de tercero, ese SaaS no forma parte del producto. El proveedor tercero tiene sus propias obligaciones bajo NIS 2.

El CRA no exige medidas de seguridad para el conjunto de las redes y sistemas de información del fabricante. Exige seguridad para los servicios remotos que forman parte del producto. La frontera es el perímetro del producto, no el perímetro de la empresa.

Tu cadena de suministro: quién hace qué bajo el CRA

El CRA pone las obligaciones principales sobre ti como fabricante, pero importadores y distribuidores también asumen deberes que influyen en cómo tu producto llega al mercado. Hay tres cosas que conviene tener claras.

Quién	Qué verifica antes del suministro	Qué hace ante una vulnerabilidad	Cuándo asume tus deberes
Importador	Marcado CE, declaración UE de conformidad, instrucciones de usuario en la lengua correcta, datos de contacto del fabricante en el producto o con él	Te informa sin demora indebida; informa directamente a las autoridades de vigilancia del mercado si el producto presenta un riesgo significativo de ciberseguridad	Cuando comercializa tu producto con su propio nombre o marca, o lo modifica sustancialmente
Distribuidor	Marcado CE, que el fabricante y el importador han cumplido su parte, que la documentación obligatoria acompaña al producto	Te informa sin demora indebida; informa directamente a las autoridades de vigilancia del mercado si el producto presenta un riesgo significativo de ciberseguridad; puede dejar de comercializar el producto	Mismo activador que para el importador

Para un fabricante esto significa tres cosas prácticas:

- Tu marcado CE, tu declaración UE de conformidad y tus instrucciones de usuario tienen que ser correctos y estar en la lengua adecuada en el momento en que un distribuidor los revise. Los socios de canal están obligados a verificarlo y pueden negarse a comercializar el producto si faltan o son incorrectos.
- Necesitas un canal de contacto claro y de baja fricción que importadores y distribuidores puedan usar para hacerte llegar vulnerabilidades a tu proceso de gestión. Lo van a usar.
- Cualquier socio que cambie la marca, comercialice tu producto con su propio nombre o marca, o lo modifique sustancialmente, se convierte en fabricante respecto de esa variante. Los deberes plenos de expediente técnico, evaluación de la conformidad, notificación y periodo de soporte se trasladan a él para esa versión. Más detalle en *Cuando otro se convierte en fabricante*, en la siguiente sección.

Modificación sustancial: cuándo procede una nueva conformidad

Una vez que tu producto está en el mercado, el CRA divide los cambios posteriores en dos campos. La mayoría son rutina y no exigen nada extra. Algunos son sustanciales. Una modificación sustancial se trata, a efectos del CRA, como un nuevo producto que se introduce en el mercado. Eso significa una nueva evaluación de la conformidad, un expediente técnico actualizado, una nueva declaración de conformidad y marcado CE sobre la nueva versión.

La prueba es corta y vive en la definición misma de modificación sustancial. Un cambio es sustancial si se cumple alguna de estas condiciones:

- **Afecta al cumplimiento** de los requisitos esenciales de ciberseguridad.
- **Modifica la finalidad prevista** para la que se evaluó el producto.

Si no aplica ninguna, el cambio no es sustancial. Documenta el razonamiento de todos modos y guárdalo en el expediente. El análisis forma parte del rastro de evidencia.

Qué no cuenta como sustancial

Dos excepciones hacen casi todo el trabajo en la práctica.

Las actualizaciones de seguridad y correcciones de errores que reducen el riesgo de ciberseguridad sin cambiar la finalidad prevista no son sustanciales. Parchear una vulnerabilidad conocida, ajustar una validación de entrada para cerrar un fallo o recompilar un componente para resolver una CVE caen de este lado de la línea.

El reacondicionamiento, el mantenimiento y las reparaciones tampoco son automáticamente sustanciales. Solo lo son si alteran la finalidad prevista o afectan al cumplimiento de los requisitos esenciales de ciberseguridad.

Los retoques menores de interfaz de usuario también quedan del lado seguro. Añadir un idioma, cambiar un juego de iconos o pulir un layout de pantalla no es por sí solo una modificación sustancial. Añadir un nuevo elemento de entrada que requiere una validación adecuada sí puede serlo.

Recambios

El CRA exime los recambios de forma estrecha y específica. Los **recambios idénticos**, fabricados con las mismas especificaciones que los componentes que sustituyen, quedan totalmente fuera del ámbito del Reglamento. Los recambios funcionales no.

Usa esta matriz para resolver el caso rápido.

Sustitución	Anfitrión introducido antes del 11 de diciembre de 2027	Anfitrión introducido el 11 de diciembre de 2027 o después
Idéntico al componente original, mismas especificaciones	Recambio fuera del ámbito del CRA. La sustitución no dispara obligaciones.	Recambio fuera del ámbito del CRA. La sustitución no dispara obligaciones.
Funcionalmente equivalente, diseño o especificación distintos	El recambio es por sí solo un producto CRA. El anfitrión no tiene obligaciones CRA, porque es anterior a la fecha de aplicación.	El recambio es un producto CRA. Evalúa si la sustitución dentro del anfitrión es una modificación sustancial del anfitrión usando la prueba de dos partes anterior.

Dos consecuencias prácticas. Primera, la excepción depende de la especificación idéntica. Un módulo inalámbrico reconstruido sobre un chipset distinto no es un recambio idéntico, aunque el cliente no note la diferencia. Segunda, el fabricante que suministra un recambio funcional carga con las obligaciones del CRA para esa pieza, sea quien sea quien fabricó el anfitrión.

Actualizaciones de software y feature flags

Las versiones de software son la fuente más habitual de dudas sobre modificación sustancial. La prueba de dos partes sigue resolviéndolas.

Un parche que corrige una vulnerabilidad no es sustancial. Un feature flag que activa una capacidad para la que el producto nunca se evaluó sí lo es. Una actualización de modelo que permite al producto decidir sobre nuevas categorías de entrada también. Si una release contiene a la vez un parche y una nueva función, evalúa la función.

El empaquetado importa menos que el fondo. Si una actualización funcional llega sola o en la misma release que un parche de seguridad es irrelevante para el análisis.

Si operas con feature flags o despliegues escalonados, el momento que cuenta es la activación para usuarios finales en producción, no el envío del binario que contiene el flag.

La decisión en la práctica

Usa esta secuencia en cada cambio antes de lanzarlo.

1. **¿El cambio modifica la finalidad prevista del producto?** Si sí: sustancial. Repite la evaluación de la conformidad para la nueva versión.
2. **¿El cambio afecta al cumplimiento de los requisitos esenciales de ciberseguridad?** Si sí: sustancial. Repite la evaluación de la conformidad para la nueva versión.
3. **En caso contrario:** no sustancial. Documenta el análisis y continúa bajo el expediente técnico existente.

Si el producto es Clase Importante o Crítico y la vía requería evaluación por tercero la primera vez, una modificación sustancial te devuelve a la misma vía. Avisa al tercero por adelantado de cualquier cambio que sea probable que sea sustancial. La autoevaluación no es una puerta trasera para reclasificar un producto Importante a posteriori.

Consecuencias cuando una modificación es sustancial

Una modificación sustancial se trata como un nuevo producto que se introduce en el mercado. Para el fabricante eso significa:

- Actualizar la documentación técnica de la versión modificada.
- Repetir la evaluación de la conformidad por la vía que exija la clase del producto.
- Emitir una nueva declaración UE de conformidad para la versión modificada.
- Volver a aplicar el marcado CE, con la nueva declaración archivada.
- Conservar la documentación de la versión anterior durante todo el periodo de retención. La nueva versión no la borra.

Para productos de software en particular, puedes acotar las actualizaciones de seguridad durante el periodo de soporte a la última versión que hayas introducido en el mercado, siempre que los usuarios de versiones anteriores puedan migrar a la última versión gratuitamente y sin hardware nuevo.

Las unidades ya vendidas bajo la conformidad anterior no se ven afectadas. La obligación recae sobre la versión modificada que se pone a disposición, no sobre unidades idénticas anteriores.

Cuando otro se convierte en fabricante

Si no eres el fabricante original y llevas a cabo una modificación sustancial, el CRA te trata como fabricante respecto de esa versión. Las obligaciones plenas de los artículos 13 y 14 pasan a ser tuyas. La misma regla se aplica si introduces el producto en el mercado con tu propio nombre o marca.

Esto atrapa más situaciones de las que los equipos suelen prever:

- Un integrador de sistemas que entrega una compilación de firmware específica para un cliente con nuevas funciones.
- Un revendedor que rebrandea un producto y cambia la finalidad prevista comercializada.
- Un proveedor de servicios que empaqueta un dispositivo de tercero con su propio firmware.

En cada caso, el actor que hizo el cambio hereda las obligaciones de fabricante para esa versión: expediente técnico, evaluación de la conformidad, notificación, gestión de vulnerabilidades y el resto. La etiqueta de "importador" o "distribuidor" deja de protegerle en el momento en que cruza cualquiera de las dos líneas.

Qué necesitas tener preparado

Usa esta sección como lista de trabajo. La guía detallada requisito por requisito aparece a continuación.

Evaluación de riesgos de ciberseguridad

Antes de introducir un producto en el mercado, necesitas una evaluación de riesgos de ciberseguridad en el expediente técnico. Es el documento que explica, con tus propias palabras, por qué el producto es seguro para lanzarse y para mantenerse en el mercado.

La evaluación debe cubrir:

- La finalidad prevista del producto y los usos que puedes prever razonablemente
- Las condiciones y el entorno en los que operará el producto
- Los datos y las funciones que necesitan protección
- Las amenazas aplicables y los controles con los que las gestionas
- El tiempo durante el que se espera que el producto esté en uso

Cómo lo estructuran la mayoría de equipos. Las metodologías creíbles convergen en los mismos movimientos: identificar los activos (datos que maneja el producto, material de seguridad como claves y credenciales, funciones cuya pérdida dañaría a los usuarios), mapear dónde reside o se mueve cada activo, modelar las amenazas por activo y entorno usando confidencialidad, integridad y disponibilidad como dimensiones, puntuar impacto y probabilidad, decidir qué riesgos residuales aceptar y cuáles mitigar, y reevaluar tras cada ronda de controles (cada nueva clave, certificado o función de autenticación es por sí mismo un nuevo activo que analizar).

Modelado de amenazas. El tercer movimiento anterior es el más técnico y tiene sus propias técnicas establecidas. STRIDE clasifica las amenazas como spoofing, tampering, repudiation, information disclosure, denial of service y elevation of privilege; muy usado, encaja con la mayoría de productos conectados. LINDDUN amplía el cuadro para productos que manejan datos personales, añadiendo linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness y non-compliance; útil cuando el régimen de protección de datos se solapa con los deberes del CRA. PASTA recorre un proceso de siete etapas desde los objetivos de negocio hasta la aceptación de riesgo residual; útil para sistemas complejos donde el cuadro de ataque dirige el diseño. Ninguna es específica del CRA y el CRA no exige ninguna. Elige la que se ajuste al perfil de exposición de tu producto.

Dónde encontrar una metodología desarrollada. El CRA no prescribe un método. La Oficina Federal de Seguridad de la Información de Alemania (BSI) publica la Guía Técnica TR-03183, la metodología de evaluación de riesgos alineada con el CRA más detallada en circulación pública. ENISA publica orientaciones más amplias sobre implementación del CRA.

Mantén la evaluación actualizada durante todo el periodo de soporte. Cuando cambie el cuadro de amenazas, los componentes o el caso de uso, la evaluación debe cambiar con ellos.

Determinación del periodo de soporte

Cada producto necesita un periodo de soporte definido y debes publicar su fecha de fin en el momento de la compra. El periodo de soporte es la ventana durante la cual gestionas vulnerabilidades, distribuyes actualizaciones de seguridad y mantienes actualizada la documentación técnica.

Cuánto debe durar

Al menos cinco años. Si se espera que el producto esté en uso menos de cinco años, el periodo de soporte debe ajustarse al tiempo de uso esperado. Si se espera que esté en uso más tiempo, el periodo de soporte debe reflejar ese uso más largo; productos como routers, sistemas operativos y controladores industriales suelen justificar más de cinco años.

Factores a considerar

Al fijar el periodo, ten en cuenta de forma proporcionada:

- Las expectativas razonables de los usuarios para el producto
- La naturaleza del producto, incluida su finalidad prevista
- Cualquier norma de la UE que ya fije una vida útil para esa categoría
- Periodos de soporte de productos comparables en el mercado
- La disponibilidad del entorno operativo del que depende el producto
- Los periodos de soporte de los componentes integrados que proporcionan funciones principales
- Cualquier orientación de ADCO o de la Comisión para la categoría del producto

El razonamiento detrás del periodo elegido debe estar en el expediente técnico. Las autoridades de vigilancia del mercado pueden pedirlo.

Qué debes publicar

Indica la fecha de fin del periodo de soporte en el momento de la compra, al menos con mes y año, en un lugar fácilmente accesible. Cuando el producto tenga una interfaz de usuario, muestra una notificación cuando alcance el fin de su periodo de soporte.

Retención de actualizaciones

Cada actualización de seguridad puesta a disposición de los usuarios durante el periodo de soporte debe permanecer disponible al menos 10 años desde su emisión, o durante el resto del periodo de soporte, lo que sea más largo.

Diligencia debida sobre componentes

Un producto está hecho de componentes. Algunos los escribiste tú, otros los compraste, otros los sacaste de un repositorio de código abierto. El CRA trata el producto como un todo a efectos de cumplimiento, así que los componentes también cuentan. Si hay una vulnerabilidad en un componente, está en tu producto. Si un componente no recibe actualizaciones de seguridad, tu producto tampoco.

Los fabricantes deben ejercer la diligencia debida sobre los componentes de terceros, incluidos los de código abierto. Los componentes no deben comprometer la ciberseguridad del producto.

Cuánta diligencia es suficiente depende del riesgo de ciberseguridad que aporte el componente. Una biblioteca que gestiona autenticación no es lo mismo que una biblioteca de renderizado de fuentes. Usa una o varias de estas comprobaciones, proporcionadas al riesgo:

1. **Comprueba el marcado CE en el componente.** Si el componente es por sí solo un producto CRA y el proveedor ha demostrado conformidad, el marcado CE va en el componente. Eso evidencia el trabajo CRA del proveedor.
2. **Revisa el historial de actualizaciones de seguridad.** Un componente que publica actualizaciones de seguridad con regularidad es mejor riesgo que uno que lleva años en silencio. Busca cadencia de versiones y un historial reciente de avisos de seguridad.
3. **Coteja el componente con bases de datos de vulnerabilidades.** La base europea de vulnerabilidades y las bases CVE públicas te dicen qué se sabe del componente. Una CVE conocida sin parche es una bandera roja.
4. **Ejecuta pruebas de seguridad adicionales.** Cuando lo anterior no baste, prueba el componente en tu contexto de integración: análisis estático, dinámico, fuzzing o una revisión de seguridad enfocada.

Para componentes integrados antes de que su propio proveedor esté plenamente bajo el CRA, sin marcado CE todavía disponible, usa las otras tres comprobaciones. La obligación de diligencia debida no se pausa porque la cadena de suministro vaya con retraso.

Evidencia a guardar en el expediente

El expediente técnico tiene que mostrar tu diligencia debida, no solo afirmarla. Conserva:

- Una lista de componentes de terceros en el producto, trazable a versiones, incluidos los de código abierto. La SBOM es el sitio natural.
- La documentación de seguridad del proveedor que revisaste: políticas de seguridad, programas de divulgación de vulnerabilidades, compromisos de periodo de soporte.
- Informes de ensayos de integración que muestren que el componente se comporta de forma segura en tu producto.
- Cláusulas de seguridad en contratos o SLAs con proveedores comerciales: plazos de notificación de vulnerabilidades, compromisos de periodo de soporte, reglas de escalado.
- Un registro de las mitigaciones a nivel de producto que añadiste cuando la diligencia debida sobre el componente reveló límites: sandboxing, permisos restringidos, validación de entrada, segmentación de red.

Cuando encuentras una vulnerabilidad en un componente

Si tu diligencia debida o tu monitorización posterior a la comercialización identifica una vulnerabilidad en un componente, debes hacer dos cosas. Primera, notificar a la persona o entidad que mantiene el componente. Si es de código abierto, eso significa el proyecto upstream. Segunda, abordar y remediar la vulnerabilidad en tu producto dentro de los mismos plazos que cualquier otra vulnerabilidad que descubras. Si has desarrollado una corrección, comparte el código o la documentación con el mantenedor, en formato legible por máquina cuando proceda.

El CRA no te permite esperar a que el mantenedor del componente actúe para proteger a tus propios usuarios. El plazo de gestión de vulnerabilidades de tu producto corre con independencia del de upstream.

Los 13 requisitos de seguridad del producto

Todo producto con elementos digitales debe cumplir trece requisitos básicos de seguridad cuando se introduce en el mercado y mantenerlos durante todo el periodo de soporte. Son el suelo de lo que significa ciberseguridad en términos de producto bajo el CRA.

Los trece requisitos son:

- Sin vulnerabilidades explotables conocidas en el momento de introducir el producto en el mercado
- Configuración segura por defecto
- Actualizaciones de seguridad, incluidas actualizaciones automáticas con opción de exclusión
- Protección frente al acceso no autorizado
- Confidencialidad de los datos almacenados, transmitidos y tratados
- Integridad de datos, firmware y configuración
- Minimización de datos
- Disponibilidad y resiliencia, incluso frente a ataques de denegación de servicio
- Sin impacto negativo en otros dispositivos o redes conectados
- Superficie de ataque limitada, incluidas interfaces externas
- Reducción del impacto de incidentes mediante mitigación de la explotación
- Registro de actividad relevante para la seguridad, con opción de exclusión para el usuario
- Supresión y portabilidad de datos segura y permanente

Cada requisito se desarrolla en detalle más adelante en la guía, con qué significa en la práctica y la evidencia que conviene guardar en el expediente.

Los 8 requisitos de gestión de vulnerabilidades

Los fabricantes también necesitan procesos de gestión de vulnerabilidades que funcionen durante todo el periodo de soporte del producto:

1. Identificar y documentar vulnerabilidades (incluye la lista de materiales de software, SBOM)
2. Gestión de riesgos y actualizaciones de seguridad a tiempo
3. Ensayos de seguridad periódicos
4. Notificación de actualizaciones de seguridad y divulgación de vulnerabilidades
5. Política de divulgación coordinada de vulnerabilidades (CVD)
6. Contacto para compartir información sobre vulnerabilidades y notificarlas
7. Mecanismos seguros de distribución de actualizaciones
8. Actualizaciones de seguridad gratuitas con mensajes de aviso

Plazos de notificación del artículo 14

Estas obligaciones se aplican desde el **11 de septiembre de 2026**. Afectan a los fabricantes de productos con elementos digitales dentro del ámbito, incluidos los productos introducidos en el mercado antes del **11 de diciembre de 2027**. Las microempresas y pequeñas empresas no están exentas con carácter general. La excepción sancionadora para pequeñas empresas es estrecha: solo se refiere al primer plazo de **alerta temprana de 24 horas**.

La Ley de Ciberresiliencia distingue tres niveles de estado de una vulnerabilidad:

- **Vulnerabilidad:** cualquier debilidad que podría explotarse
- **Vulnerabilidad explotable:** una debilidad que puede usarse en condiciones reales
- **Vulnerabilidad explotada activamente:** una vulnerabilidad cuyo uso en un ataque se ha confirmado

Cuándo empieza el reloj

No empiezas el reloj en el momento en que llega una señal. El reloj arranca una vez que has hecho una evaluación inicial y tienes un grado razonable de certeza de que una vulnerabilidad de tu producto se está explotando activamente, o de que un incidente grave ha comprometido la seguridad del producto. El énfasis está en la evaluación inicial rápida, no en esperar a cerrar la investigación completa. Si un cliente, investigador, autoridad u otro tercero te traslada una posible incidencia, evalúala sin demora y arranca el reloj en cuanto esa evaluación te dé esa certeza razonable.

Cuando detectes una **vulnerabilidad explotada activamente**, se aplica este calendario de notificación:

Plazo	Qué se exige	Dónde notificar
En 24 horas	Notificación de alerta temprana de explotación activa	ENISA a través del CSIRT nacional
En 72 horas	Notificación de vulnerabilidad: producto afectado, naturaleza general del exploit y de la vulnerabilidad, mitigaciones, medidas correctivas que pueden aplicar los usuarios y marcado de sensibilidad cuando proceda	ENISA a través del CSIRT nacional
A más tardar 14 días después de que esté disponible una medida correctiva o mitigadora	Informe final: descripción de la vulnerabilidad, gravedad, impacto, información disponible sobre actores maliciosos y detalles de la actualización de seguridad u otras medidas correctivas	ENISA a través del CSIRT nacional

Cuando detectes un **incidente grave** que afecte a la seguridad del producto, se aplica este calendario de notificación:

Plazo	Qué se exige	Dónde notificar
En 24 horas	Notificación de alerta temprana, incluida la indicación de si se sospecha que el incidente se debe a actos ilícitos o maliciosos	ENISA a través del CSIRT nacional
En 72 horas	Notificación de incidente: naturaleza del incidente, evaluación inicial, mitigaciones, medidas correctivas que pueden aplicar los usuarios y marcado de sensibilidad cuando proceda	ENISA a través del CSIRT nacional
En el plazo de un mes desde la notificación de incidente de 72 horas	Informe final: descripción detallada del incidente, gravedad, impacto, amenaza probable o causa raíz, y medidas de mitigación aplicadas o en curso	ENISA a través del CSIRT nacional

Las notificaciones se actualizan a medida que sabes más

Las presentaciones a 24 horas, 72 horas y 14 días o un mes son fases de la misma notificación, no archivos separados. Cada fase añade la información que aún no estaba disponible en la anterior. El CSIRT designado coordinador también puede pedir una actualización intermedia en cualquier momento. No tienes que repetir información que ya hayas facilitado.

Las notificaciones se presentan a través de la **Plataforma Única de Notificación del CRA**, enrutadas por el equipo de respuesta a incidentes de seguridad informática (CSIRT) nacional del Estado miembro principal del fabricante, con acceso simultáneo para ENISA.

Informar a tus usuarios

Tras tener conocimiento, debes informar a los usuarios afectados por la vulnerabilidad o incidente y, cuando proceda, a todos los usuarios, de cualquier medida de mitigación de riesgo y de las medidas correctivas que puedan aplicar. Esto no es lo mismo que la divulgación pública. El deber es hacer llegar la información a los

usuarios que la necesitan para protegerse, de forma proporcionada al riesgo. Para productos usados en entornos sensibles o esenciales, limita la información técnica detallada a los clientes afectados mientras la vulnerabilidad esté sin mitigar; el detalle público prematuro puede facilitar la explotación.

Una vez que la vulnerabilidad se ha remediado o mitigado, puede ser apropiada una divulgación más amplia para ayudar a los usuarios a verificar que sus productos ya no están afectados y elevar la conciencia general. Mantén el nivel de detalle y los tiempos proporcionados al riesgo residual. Si no informas a los usuarios a tiempo, el CSIRT puede intervenir y facilitar la información por sí mismo cuando lo considere proporcionado y necesario.

Vulnerabilidad explotada activamente	
24 horas	notificación de alerta temprana
72 horas	notificación de vulnerabilidad
14 días tras la medida correctiva	informe final

Incidente grave	
24 horas	notificación de alerta temprana
72 horas	notificación de incidente
un mes tras la notificación de 72 horas	informe final

Acción correctiva cuando un producto no es conforme

Si sabes, o tienes motivos para creer, que un producto que has introducido en el mercado, o uno de tus procesos, no es conforme con los requisitos esenciales de ciberseguridad del CRA, debes actuar de inmediato. El deber corre desde la introducción en el mercado y durante todo el periodo de soporte.

Las tres opciones

1. **Poner en conformidad.** Corrige el producto o el proceso. Para productos de software esto suele ser una actualización de seguridad o un cambio de proceso. Aplica la corrección a las versiones soportadas.
2. **Retirar.** Deja de poner el producto a disposición en el mercado. Sácalo de tu cadena de suministro y de cualquier minorista, integrador o revendedor que tenga existencias.
3. **Recuperar.** Recupera el producto de los usuarios que ya lo tienen. Usa esta vía cuando el riesgo de ciberseguridad para los usuarios sea significativo y una corrección o retirada por sí solas no basten.

La elección es proporcionada al riesgo, no una secuencia fija. Una vulnerabilidad parcheable con una corrección que funciona suele significar *poner en conformidad*. Un producto que no puede corregirse con seguridad sobre el terreno suele significar *retirar* y, cuando está en uso activo con un riesgo significativo, *recuperar*.

Qué más debes hacer

- **Notificar dentro de la cadena del artículo 14** cuando la no conformidad sea una vulnerabilidad explotada activamente o un incidente grave. El calendario de notificación está más arriba.
- **Informar a los usuarios** de la no conformidad y de las medidas correctivas que ellos mismos puedan aplicar. Las reglas de proporcionalidad están en *Informar a tus usuarios*, más arriba.
- **Cooperar** con cualquier solicitud motivada de una autoridad de vigilancia del mercado, lo que incluye facilitar la documentación técnica en una lengua que puedan leer.
- **Preservar la evidencia.** Guarda los registros que muestran qué encontraste, cuándo lo encontraste, qué hiciste al respecto y cómo te comunicaste con usuarios y autoridades. La documentación técnica y la declaración UE de conformidad deben permanecer disponibles al menos 10 años desde la introducción en el mercado, o durante todo el periodo de soporte, lo que sea más largo.

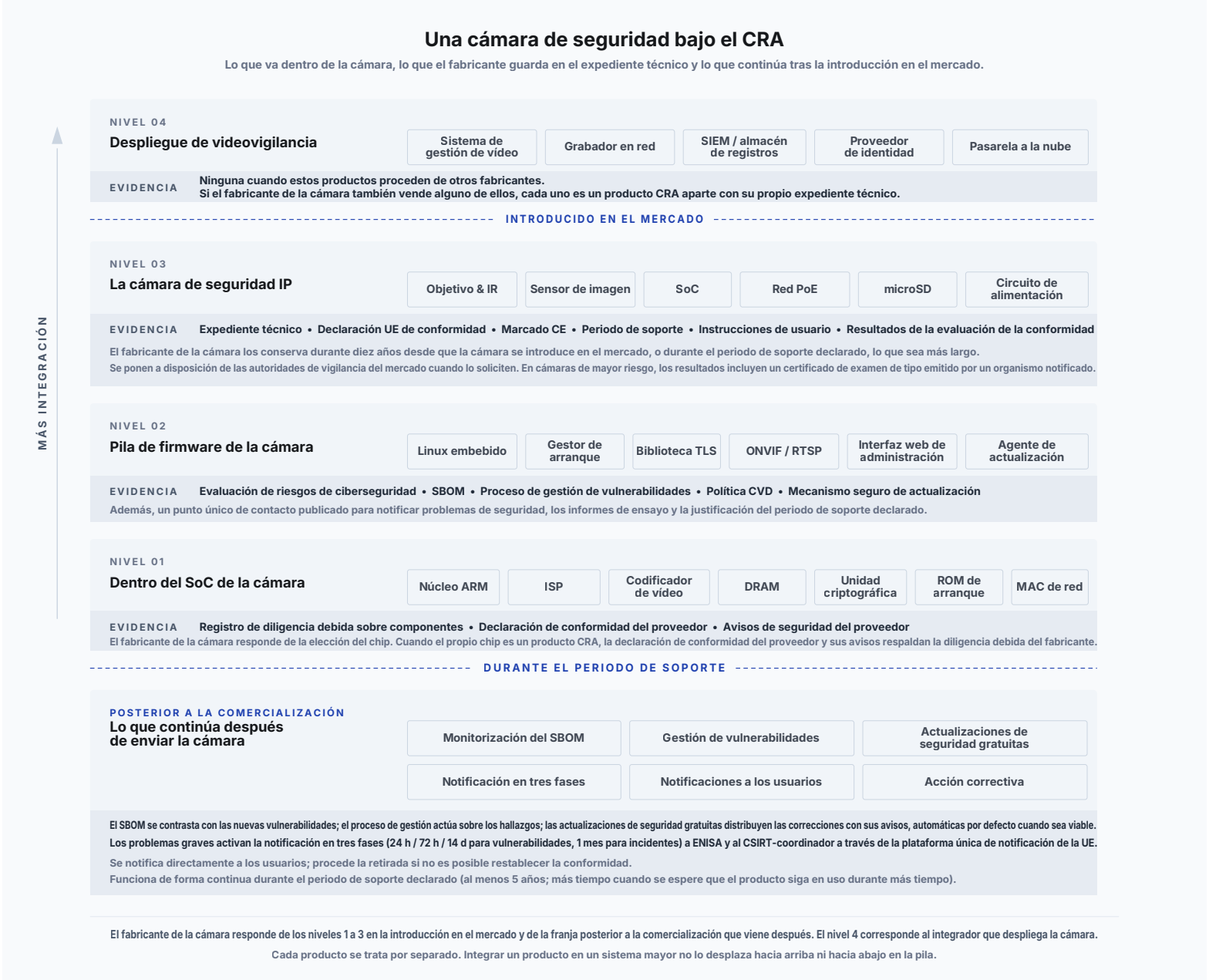
Requisitos de documentación del producto

La documentación debe conservarse durante **al menos 10 años** después de que el producto se haya introducido en el mercado, o durante **todo el periodo de soporte**, lo que sea más largo. A nivel de resumen, la documentación técnica necesita ocho familias de evidencia:

1. Descripción general del producto
2. Detalles de diseño, desarrollo y producción (incluida la SBOM)
3. Evaluación de riesgos de ciberseguridad
4. Determinación del periodo de soporte
5. Normas armonizadas y especificaciones aplicadas
6. Informes de ensayo
7. Declaración UE de conformidad
8. SBOM completa (a petición de las autoridades de vigilancia del mercado)

Checklist de la vía de evaluación de la conformidad

Usa la tabla de clasificación anterior para identificar la vía. Después conserva la decisión de ruta en el expediente técnico junto con las normas, especificaciones, esquema de certificación o evidencia de organismo notificado utilizada para justificarla.



Un ejemplo resuelto. La misma estructura por niveles se aplica a cualquier producto con elementos digitales, no solo a las cámaras de seguridad.

Los requisitos de seguridad del producto

a. Sin vulnerabilidades explotables conocidas en el momento de introducirlo en el mercado

No lances un producto con vulnerabilidades explotables conocidas públicamente que sigan sin tratar. Una vulnerabilidad conocida puede venir de una base de datos pública, un aviso de proveedor, una comunicación de cliente o tu propio registro interno.

Para cumplir este requisito:

- Comprueba bases de datos de vulnerabilidades, incluidas Common Vulnerabilities and Exposures (CVE), antes de cada versión
- Usa pruebas estáticas y dinámicas de seguridad de aplicaciones (SAST/DAST) en tu pipeline de compilación
- Realiza análisis de dependencias para todos los componentes de terceros y de código abierto
- Documenta tu decisión de aceptación del riesgo o mitigación para cada problema identificado

b. Configuración segura por defecto

El producto debe ser seguro en su estado por defecto. Desactiva servicios innecesarios, evita credenciales débiles por defecto y mantén cualquier modo de puesta en marcha inseguro durante el menor tiempo posible y bajo control. La obligación de configuración segura por defecto puede modificarse para productos a medida suministrados a usuarios empresariales mediante acuerdo escrito, siempre que se mantenga la posibilidad de restablecer el producto a su estado original.

Para cumplir este requisito:

- Desactiva puertos de acceso remoto e interfaces de depuración en las compilaciones por defecto
- Exige mecanismos sólidos de autenticación por defecto
- Restringe las funciones administrativas solo a usuarios autorizados
- Implementa un restablecimiento seguro de fábrica que devuelva todos los ajustes y firmware a un estado seguro conocido y elimine los datos de usuario

c. Actualizaciones de seguridad, incluidas actualizaciones automáticas con opción de exclusión

El producto necesita un mecanismo de parcheo capaz de gestionar problemas de seguridad tras el despliegue. Cuando las actualizaciones automáticas sean adecuadas, actívalas por defecto y ofrece a los usuarios una forma clara de aplazarlas o desactivarlas.

Para cumplir este requisito:

- Implementa firma criptográfica y verificación de integridad para los paquetes de actualización
- Proporciona prevención de reversión y registro de eventos de actualización
- Crea sistemas de notificación que avisen a los usuarios de actualizaciones pendientes
- Permite aplazar o desactivar actualizaciones automáticas mediante una interfaz de configuración clara

d. Protección frente al acceso no autorizado

Los controles de acceso deben proteger tanto las interfaces locales como las remotas. El objetivo es impedir que usuarios no autorizados alcancen funciones, datos, configuración o superficies de administración.

Para cumplir este requisito:

- Exige políticas de complejidad de contraseñas y credenciales sólidas por defecto
- Implementa autenticación multifactor (MFA) cuando proceda
- Aplica control de acceso basado en roles (RBAC) y gestión de caducidad de sesión
- Registra intentos de acceso fallidos, usa detección de anomalías para señalar actividad no autorizada y deriva esos eventos para su revisión y notificación

e. Confidencialidad de los datos almacenados, transmitidos y tratados

Los datos sensibles necesitan protección en reposo, en tránsito y durante el tratamiento.

Para cumplir este requisito:

- Usa algoritmos de cifrado estandarizados, por ejemplo AES-256 para datos en reposo y TLS para datos en tránsito
- Aplica prácticas seguras de gestión de claves
- Segrega los datos confidenciales de componentes del sistema no críticos
- Mantén registros de auditoría para todos los eventos de acceso a datos

f. Integridad de datos, firmware y configuración

Este requisito cubre el propio sistema (firmware, software, archivos de configuración) y los datos que gestiona (mediciones, comandos de control, entradas de usuario).

Para cumplir este requisito:

- Implementa arranque seguro y firmware firmado para garantizar que solo se ejecuta código de confianza
- Usa verificación en tiempo de ejecución para detectar e informar de intentos de manipulación
- Aplica hashes criptográficos y firmas digitales para proteger la integridad de los datos
- Construye infraestructura capaz de generar, distribuir y verificar claves criptográficas entre sistemas o límites organizativos

g. Minimización de datos

Recoge y trata solo los datos necesarios para la finalidad prevista del producto. Esto se aplica a datos personales y a datos técnicos.

Para cumplir este requisito:

- Realiza evaluaciones de impacto de privacidad o ejercicios de protección de datos desde el diseño para identificar flujos de datos innecesarios
- Elimina o convierte en opcional cualquier telemetría, diagnóstico o recogida de datos en segundo plano que no se use
- Implementa ajustes configurables de recogida de datos para que la recogida ampliada pueda activarse o desactivarse según el contexto

h. Disponibilidad y resiliencia, incluso frente a ataques de denegación de servicio

Durante incidentes o ataques, las funciones clave del producto deben seguir disponibles o fallar de forma controlada.

Para cumplir este requisito:

- Implementa interruptores de circuito, lógica de reintento, mecanismos de respaldo y temporizadores de vigilancia
- Aplica límites de recursos para evitar el agotamiento de recursos
- Usa limitación de tasa y validación de entradas para proteger frente a escenarios de denegación de servicio
- Aplica filtrado a nivel de red para bloquear intentos de sobrecarga

i. Sin impacto negativo en otros dispositivos o redes conectados

El producto no debe alterar otros sistemas del mismo entorno. Debe comportarse de forma predecible y evitar un uso excesivo de recursos compartidos.

Para cumplir este requisito:

- Implementa gestión de tráfico y limita el uso de broadcast o multicast
- Garantiza el cumplimiento de las especificaciones de los protocolos de comunicación
- Usa automonitorización para detectar y evitar comportamientos disruptivos como inundación de red o agotamiento de recursos

j. Superficie de ataque limitada, incluidas interfaces externas

Minimiza los puntos de entrada y la funcionalidad expuesta. Esto incluye puertos físicos, interfaces inalámbricas, APIs, servicios de depuración y componentes de software innecesarios.

Para cumplir este requisito:

- Desactiva servicios, puertos e interfaces no usados en compilaciones de producción
- Endurece los valores por defecto del sistema y limita los privilegios de usuario
- Modulariza las arquitecturas de software para aislar componentes entre sí
- Aplica principios de diseño seguro de software y realiza modelado de amenazas para identificar y eliminar exposición innecesaria

k. Reducción del impacto de incidentes mediante mitigación de la explotación

Asume que algunos ataques tendrán éxito. El diseño del producto debe limitar hasta dónde puede propagarse el daño.

Para cumplir este requisito:

- Separa componentes del sistema y ejecútalos en entornos aislados mediante aislamiento tipo sandbox o contenedorización
- Exige separación de privilegios para que las funciones críticas se ejecuten con los permisos mínimos necesarios
- Diseña el producto para que el compromiso de un componente no permita a un atacante controlar todo el sistema

l. Registro de actividad relevante para la seguridad con opción de exclusión para el usuario

Registra actividad relevante para la seguridad, como intentos de acceso y modificaciones de datos, para poder monitorizarla y auditarla. Los usuarios necesitan un mecanismo de exclusión cuando la Ley de Ciberresiliencia lo exige.

Para cumplir este requisito:

- Implementa registros estructurados, por ejemplo registros en JSON con marcas de tiempo
- Proporciona almacenamiento local de logs con rotación y opciones de envío remoto
- Monitoriza eventos como intentos de inicio de sesión, cambios de configuración y actualizaciones de software para detectar anomalías
- Ofrece un mecanismo claro de cara al usuario para desactivar el registro cuando esté permitido

m. Supresión y portabilidad de datos segura y permanente

Los usuarios necesitan una forma práctica de eliminar datos y ajustes de manera permanente. Cuando los datos puedan transferirse a otro producto o sistema, la transferencia debe ser segura.

Para cumplir este requisito:

- Implementa una función de borrado seguro que sobrescriba regiones de almacenamiento o elimine criptográficamente claves
- Usa canales autenticados y cifrados para transferencias de portabilidad de datos y evitar exposición durante la transferencia

Los requisitos de gestión de vulnerabilidades

1. Identificar y documentar vulnerabilidades

Necesitas saber qué componentes de software contiene el producto y qué vulnerabilidades conocidas les afectan. Una lista de materiales de software (SBOM) te da ese inventario legible por máquina.

Para cumplir este requisito:

- Integra la generación de SBOM directamente en tu pipeline de CI/CD para que cada compilación produzca un inventario de componentes actualizado
- Usa formatos establecidos como CycloneDX, SPDX o SWID para la interoperabilidad
- Ejecuta análisis automatizado de vulnerabilidades contra listados CVE y bases de datos como CISA KEV y ENISA EUVD
- Mantén la SBOM como parte de tu documentación técnica durante todo el periodo de soporte y facilítala a las autoridades de vigilancia del mercado cuando la soliciten

2. Gestión de riesgos y actualizaciones de seguridad a tiempo

Cuando se encuentren vulnerabilidades, corrígelas rápido y entrega actualizaciones de seguridad. Cuando sea posible, separa los parches de seguridad de las actualizaciones funcionales para que las correcciones críticas puedan instalarse con rapidez.

Para cumplir este requisito:

- Diseña tu mecanismo de actualización para que las correcciones de seguridad puedan desplegarse sin exigir una actualización completa del sistema
- Estructura el software y el firmware para que los componentes críticos puedan parchearse de forma independiente
- Entrega actualizaciones por canales seguros con comprobaciones de integridad
- Mantén registros de las actividades de actualización para respaldar la trazabilidad y demostrar cumplimiento

3. Ensayos de seguridad periódicos

Los ensayos de seguridad no son un ejercicio puntual. Prueba los productos durante todo el ciclo de vida a medida que cambian las amenazas, las dependencias y el comportamiento del producto. Deja que la evaluación de riesgos determine el tipo y la frecuencia de los ensayos.

Para cumplir este requisito:

- Realiza pruebas de penetración para simular ataques reales
- Aplica análisis estático y dinámico de código para identificar debilidades de seguridad
- Usa fuzz testing para descubrir fallos de gestión de entradas
- Programa y documenta formalmente revisiones de código de seguridad y revisiones de arquitectura, especialmente tras cambios significativos de diseño o funcionalidad

4. Recepción de vulnerabilidades, política CVD y avisos

Cubre los deberes de recepción, divulgación coordinada y avisos (puntos 4, 5 y 6 del resumen anterior), que en la práctica funcionan como un único flujo de trabajo.

El CRA nombra tres requisitos separados sobre cómo se comunican las vulnerabilidades: una vía para que la gente notifique problemas, una política de divulgación coordinada y un aviso cuando publicas una corrección. Esto es lo que pide cada deber.

Recepción

Da a quien notifica una vía clara y de baja fricción. Publica un método de contacto visible para notificación de vulnerabilidades (correo dedicado o formulario web). Admite comunicación segura, por ejemplo publicando una clave PGP. El deber cubre las notificaciones sobre tu propio producto y sobre los componentes de terceros que contiene.

Triaje

Acusa cada notificación, regístrala en un sistema de seguimiento, asígnala para revisión y resuélvela dentro de plazos definidos. Envía confirmación y actualizaciones de estado a quien notifica. Cuando el problema esté en un componente de terceros, encamínalo al mantenedor upstream en paralelo a tu propia remediación.

Política de divulgación coordinada de vulnerabilidades

Publica una política de CVD que fije expectativas para quienes notifican y para los socios: método de contacto, tiempos de respuesta esperados, a qué te comprometes, qué pides a cambio. Coordina la divulgación para proteger a los usuarios reconociendo a la vez la aportación de quien notifica.

Avisos al publicar la corrección

Una vez que la corrección esté disponible, publica un aviso del problema resuelto. Incluye el identificador CVE, las versiones de producto afectadas, una valoración de gravedad estandarizada (por ejemplo CVSS) e información clara y accesible sobre qué deben hacer los usuarios. Redacta en un lenguaje accesible tanto para administradores técnicos como para usuarios no técnicos.

Divulgación pública diferida

Solo puedes diferir la divulgación pública cuando tengas una razón debidamente justificada de que los riesgos de ciberseguridad de la divulgación inmediata pesan más que sus beneficios, y solo hasta que los usuarios hayan tenido la oportunidad de aplicar la corrección. Documenta el razonamiento.

5. Mecanismos seguros de distribución de actualizaciones

El mecanismo de actualización debe ser fiable y resistente a manipulaciones. Cuando las actualizaciones automáticas sean técnicamente viables, reducen el tiempo durante el que los usuarios permanecen expuestos.

Para cumplir este requisito:

- Transmite actualizaciones por canales seguros y verifícalas mediante firmas digitales
- Aplica actualizaciones de forma que se eviten instalaciones incompletas o corruptas
- Usa actualizaciones diferenciales o modulares para reducir interrupciones y entregar correcciones a los sistemas con más rapidez
- Mantén registros de actualización para que usuarios o administradores puedan verificar el estado de actualización

6. Actualizaciones de seguridad gratuitas con mensajes de aviso

Entrega actualizaciones de seguridad con rapidez y sin coste adicional, salvo que exista un acuerdo separado para productos empresariales hechos a medida. Cada actualización necesita un mensaje de aviso claro que diga a los usuarios qué ha cambiado y qué hacer.

Para cumplir este requisito:

- Mantén un sistema de distribución que pueda notificar directamente a los usuarios o aplicar actualizaciones automáticamente, según el contexto del producto
- Redacta mensajes de aviso comprensibles tanto para usuarios técnicos como no técnicos
- Incluye información de gravedad en los mensajes de aviso cuando sea pertinente
- Indica a los usuarios qué acción tomar: aplicar la actualización, cambiar una configuración o vigilar síntomas de compromiso
- Difunde las actualizaciones de seguridad sin demora una vez que estén disponibles, para que los usuarios no queden expuestos mientras la corrección ya existe
- Publica los avisos a través de un canal controlado por el fabricante y enlázalos desde la página de soporte del producto

Los deberes de gratuidad y de sin demora corren durante toda la duración del periodo de soporte declarado. La excepción para productos a medida cambia solo la base comercial; los mensajes de aviso siguen aplicando.

Qué incluye el expediente técnico

Documentación técnica

La documentación técnica es la prueba central del cumplimiento del CRA. Debe cubrir las medidas de diseño, técnicas y procedimentales usadas para cumplir los requisitos esenciales de ciberseguridad. Debe existir **antes de la introducción en el mercado** y mantenerse actualizada durante todo el **periodo de soporte**.

Evidencia del expediente técnico a lo largo del flujo de ingeniería

Paso 1	**Delimitar y clasificar**	Finalidad del producto, uso previsto, decisión de introducción en el mercado, clase de producto, ruta de normas.
Paso 2	**Arquitectura y riesgo**	Arquitectura, conexiones de datos, condiciones de uso, evaluación de riesgos, mitigaciones.
Paso 3	**Componentes y SBOM**	SBOM legible por máquina, componentes de terceros, entradas de proveedores, seguimiento de vulnerabilidades.
Paso 4	**Compilar, probar, actualizar**	Valores seguros por defecto, hardening, informes de ensayo, mecanismo seguro de actualización, avisos.
Paso 5	**Lanzar y dar soporte**	Instrucciones de usuario, declaración UE, evidencia CE, justificación del soporte, registros de actualización.

El expediente técnico tiene ocho componentes obligatorios. Juntos explican **qué es el producto**, **cómo se construyó y probó**, **qué riesgos se consideraron**, **qué normas se aplicaron** y **cómo se le dará soporte** una vez en el mercado. No tienes que copiar los encabezados legales, pero cada tema debe quedar cubierto.

N.º	Componente	Qué debe contener
1	Descripción general del producto	Finalidad prevista y funciones, versiones de software pertinentes, fotos o ilustraciones (para hardware), información e instrucciones de usuario
2	Detalles de diseño, desarrollo y producción	Descripción de la arquitectura (componentes e interacciones), lista de materiales de software (SBOM), procesos de gestión de vulnerabilidades (política CVD, punto de contacto, mecanismos seguros de actualización), procesos de producción y monitorización incluida la validación
3	Evaluación de riesgos de ciberseguridad	Análisis documentado de los riesgos del producto, explicación de cómo se aplica cada requisito esencial de ciberseguridad al producto, mitigación de los riesgos identificados
4	Determinación del periodo de soporte	Documentación de los factores usados para fijar el periodo de soporte, como expectativas de usuario, productos comparables y orientación legal
5	Normas armonizadas y especificaciones aplicadas	Lista de normas armonizadas, especificaciones comunes o esquemas de certificación de la UE aplicados; indicación de si se aplican total o parcialmente; soluciones alternativas cuando no se apliquen normas
6	Informes de ensayo	Evidencia de conformidad tanto del producto como de los procesos de gestión de vulnerabilidades
7	Declaración UE de conformidad	Copia de la declaración que vincula el expediente técnico con las obligaciones de marcado CE
8	SBOM completa (a petición)	Las autoridades de vigilancia del mercado pueden exigir la SBOM completa para verificar el cumplimiento

Un único expediente técnico consolidado puede cubrir el CRA y otra legislación de la UE aplicable, por ejemplo la Directiva de Equipos Radioeléctricos o el ESPR, siempre que incluya todas las obligaciones aplicables.

Declaración UE de conformidad

La declaración UE de conformidad es la declaración formal del fabricante de que el producto cumple los requisitos de ciberseguridad aplicables del CRA. Cada declaración debe incluir:

- Nombre, tipo e identificadores únicos del producto
- Nombre y dirección del fabricante (o representante autorizado)
- Declaración de responsabilidad exclusiva del proveedor
- Descripción del producto que garantice su trazabilidad, opcionalmente con imagen
- Declaración explícita de conformidad con la legislación de la Unión pertinente
- Referencias a normas armonizadas, especificaciones o certificaciones usadas
- Datos de cualquier organismo notificado implicado (nombre, número, procedimiento, número de certificado)
- Bloque de firma: lugar, fecha, nombre, función y firma del firmante

Una vez firmada, la declaración es jurídicamente vinculante y confirma la plena responsabilidad del fabricante sobre el cumplimiento de ciberseguridad.

Se permite una declaración simplificada para su uso en embalajes o manuales, con esta forma: "Por la presente, [fabricante] declara que el producto [tipo/designación] cumple con el Reglamento (UE) 2024/2847. El texto completo de la declaración UE de conformidad está disponible en: [dirección web]." Esta forma simplificada mantiene la transparencia y reduce la carga documental, y resulta especialmente útil para pequeños fabricantes o carteras multiproducto.

Información e instrucciones de usuario

La información e instrucciones de usuario son una condición para la introducción lícita en el mercado. Los fabricantes deben mantenerlas disponibles durante **al menos 10 años** o durante **todo el periodo de soporte**. Importadores y distribuidores deben comprobar que las instrucciones existen, están actualizadas y se facilitan en la lengua de la UE correcta antes de introducir o suministrar el producto.

Las instrucciones de usuario deben contener:

- Identidad y datos de contacto del fabricante
- Un punto único de contacto para notificación de vulnerabilidades
- Identificación del producto, finalidad prevista y contexto de uso seguro
- Riesgos cibernéticos conocidos o previsibles
- Enlace a la declaración UE de conformidad
- Condiciones de soporte y fecha clara de fin de soporte
- Instrucciones de seguridad paso a paso para configuración, actualizaciones, uso seguro, retirada del servicio y, si procede, integración y acceso a SBOM

Cómo elegir la vía correcta de evaluación de la conformidad

Módulo A: autoevaluación

El módulo A (control interno) te permite autocertificar que tu producto cumple los requisitos esenciales de ciberseguridad, asumiendo plena responsabilidad tanto de su diseño como de su producción. Esta vía está disponible para fabricantes de productos por defecto (no clasificados). También está disponible para productos Importante Clase I solo cuando las normas armonizadas, especificaciones comunes o esquemas europeos de certificación de ciberseguridad pertinentes estén disponibles y se apliquen según lo exigido por las reglas de ruta del CRA.

Bajo módulo A, debes:

- Preparar documentación técnica completa
- Detallar el diseño del producto, los procesos de producción, los mecanismos de ciberseguridad y los procedimientos de gestión de vulnerabilidades
- Mantener responsabilidad continua por el cumplimiento durante todo el ciclo de vida del producto
- Implementar un plan de actualizaciones de seguridad y gestión de vulnerabilidades durante la vida operativa del producto
- Mantener registros disponibles durante al menos 10 años

Módulos B y C: evaluación centrada en el producto

Los módulos B y C se aplican cuando se exige verificación por tercero de un tipo específico de producto. Se aplican a productos Importante Clase I cuando el fabricante no ha aplicado, ha aplicado solo parcialmente o no puede aplicar normas armonizadas, especificaciones comunes o esquemas de certificación pertinentes. Para productos Importante Clase II, el fabricante debe usar módulo B+C, módulo H o un esquema europeo de certificación de ciberseguridad aplicable con nivel de garantía al menos "sustancial".

Módulo B (examen UE de tipo): un organismo notificado examina una muestra representativa del producto y la documentación técnica relacionada. Verifica el cumplimiento de todos los requisitos esenciales de ciberseguridad y emite un certificado de examen UE de tipo cuando el diseño del producto cumple los criterios del CRA.

Módulo C (conformidad con el tipo, control de producción): el fabricante garantiza que todas las unidades de producción se ajustan al tipo aprobado certificado bajo módulo B. El fabricante coloca el marcado CE, emite la declaración UE de conformidad y mantiene registros disponibles durante al menos 10 años. Juntos, los módulos B y C garantizan que un modelo de producto específico es técnicamente conforme y que cada lote de producción sigue siendo coherente con el diseño aprobado.

Módulo H: evaluación centrada en el proceso (garantía de calidad total)

El módulo H (garantía de calidad total) se centra en todo el sistema interno de calidad del fabricante, no en ensayos individuales de producto. Está disponible para productos Importante Clase I y Clase II. Los productos críticos usan la vía de certificación cuando se cumplen las condiciones pertinentes; cuando no se cumplen, usan las mismas vías disponibles para productos Importante Clase II.

Bajo módulo H, debes:

- Establecer y mantener un sistema de calidad que cubra diseño, desarrollo, producción, ensayos y gestión de vulnerabilidades para toda la categoría de producto
- Presentar el sistema de calidad a un organismo notificado para evaluación y aprobación
- Aceptar vigilancia continua (auditorías, inspecciones y revisiones de procesos) por parte del organismo notificado para verificar el cumplimiento continuo

Una vez aprobado, puedes emitir declaraciones de conformidad para todos los productos fabricados bajo ese sistema de calidad, sin repetir el examen del organismo notificado para cada tipo de producto individual.

La diferencia clave entre vías:

- Módulos B+C: se centran en el producto. Se prueba y certifica un tipo de producto representativo.
- Módulo H: se centra en el proceso. Se certifica y monitoriza todo el sistema de diseño y producción del fabricante.

La Ley de Ciberresiliencia dentro del marco normativo de la UE

El CRA no está aislado. La pregunta para un fabricante es práctica: dónde te ahorra trabajo tu evidencia CRA bajo otro régimen de la UE, y dónde sigues teniendo obligaciones separadas que correr en paralelo.

Dónde tu trabajo CRA se puede reutilizar

- **Sistemas de IA de alto riesgo (Ley de IA, Reglamento 2024/1689).** Si tu producto es un sistema de IA de alto riesgo en el ámbito del CRA, cumplir los requisitos esenciales de ciberseguridad del CRA se considera satisfacer los requisitos de ciberseguridad de la Ley de IA en la medida cubierta por tu declaración UE de conformidad. El procedimiento de evaluación de la conformidad se enruta por el régimen de la Ley de IA por regla general, con una excepción para los productos CRA Importantes y Críticos. La evaluación de riesgos de ciberseguridad del CRA debe tener en cuenta riesgos específicos de la IA como el envenenamiento de datos y los ataques adversarios.
- **Evaluación de riesgos consolidada con otra norma de la Unión.** El CRA permite expresamente que la evaluación de riesgos de ciberseguridad forme parte de una evaluación de riesgos más amplia exigida por otro acto jurídico de la Unión, cuando el producto cae bajo ambos regímenes. Un único artefacto de evaluación, dos usos regulatorios.
- **Un expediente técnico para varios regímenes.** Como ya se indicó en la sección del expediente técnico, un único expediente técnico consolidado puede cubrir el CRA junto con otra legislación aplicable de la Unión, siempre que se aborden las obligaciones de cada régimen. Útil cuando el mismo producto ya necesita documentación bajo la Directiva de Equipos Radioeléctricos, el Reglamento de Ecodiseño para Productos Sostenibles u otra norma de producto.
- **Definiciones compartidas de reacondicionamiento, mantenimiento y reparación.** El CRA importa estas definiciones del Reglamento de Ecodiseño para Productos Sostenibles. Cuando analices si una operación de servicio cuenta como modificación sustancial, las definiciones del Ecodiseño son la referencia, no un término específico del CRA.

Dónde quedan obligaciones separadas

- **Todo lo demás de la Ley de IA.** La ciberseguridad es solo una porción de la Ley de IA. La clasificación de riesgos, la transparencia, la gobernanza de conjuntos de datos, la supervisión humana, la monitorización posterior a la comercialización del comportamiento de la IA y el resto son deberes de la Ley de IA que el CRA no aborda. La ciberseguridad conforme con el CRA no es una presunción de conformidad global con la Ley de IA.
- **Ecodiseño y contenido del pasaporte digital de producto.** Los requisitos de Ecodiseño sobre eficiencia energética, durabilidad, puntuación de reparabilidad y el contenido de sostenibilidad del pasaporte digital de producto no son ámbito del CRA. El rastro de evidencia del CRA puede convivir con el trabajo de Ecodiseño pero no lo sustituye.
- **Derechos de acceso a datos IoT del Data Act.** El Data Act otorga a los usuarios derechos contractuales para acceder, compartir y transferir los datos que generan sus productos conectados. El CRA cubre la seguridad de esos datos; no fija el régimen de derechos de acceso. Obligación distinta, evidencia distinta.
- **Responsabilidad por productos defectuosos.** La Directiva de Responsabilidad por Productos (2024/2853) mantiene la responsabilidad objetiva sobre el fabricante por daños causados por productos defectuosos. El CRA señala que la falta de actualizaciones de seguridad posteriores a la comercialización puede ser el defecto que dispare la responsabilidad. Tus contratos, seguros y guías de incidentes deben cubrir esta exposición de forma independiente de la conformidad CRA.

Cómo ayuda CRA Evidence

CRA Evidence convierte las obligaciones de la Ley de Ciberresiliencia de la UE en evidencia de producto verificable, combinando una plataforma de cumplimiento con consultoría técnica.

Plataforma

Un único lugar para gestionar la evidencia detrás de la preparación CRA:

- **Inventario SBOM y componentes:** registros CycloneDX, SPDX y HBOM para versiones y lanzamientos de producto
- **Automatización de evidencia CI/CD:** flujos CLI y API para escaneos, cargas de SBOM, puertas de release y registros de auditoría
- **SBOM firmada y procedencia:** evidencia versionada, atestaciones de proveedores y registros de diligencia debida
- **Operaciones de vulnerabilidades:** CISA KEV, EPSS, VEX, monitorización, triaje y flujos de notificación
- **Expediente técnico y evidencia CE:** registros de declaración UE, historial de retención y pasaportes de cumplimiento enlazados por QR

Consultoría técnica

Soporte enfocado para convertir obligaciones CRA en decisiones de ingeniería sobre producto, arquitectura, release y proveedores.

- **Sprint de preparación técnica:** revisión de brechas frente a los requisitos esenciales, recomendaciones de arquitectura y plan de acción priorizado
- **Dirección del programa CRA:** modelo de responsabilidad, seguimiento de obligaciones, hitos de evidencia y mantenimiento del expediente técnico
- **Plan de respuesta ante autoridades e incidentes:** flujos de notificación, guías de consulta, comunicaciones a usuarios y preparación de paquetes de evidencia
- **Alineación regulatoria:** conectar evidencia CRA con Data Act, ESPR, AI Act, RED y requisitos sectoriales
- **Talleres técnicos:** sesiones remotas o presenciales con producto, ingeniería, seguridad, cumplimiento y proveedores

Independiente de herramientas: CRA Evidence se integra con CycloneDX, SPDX, Grype, Trivy, pipelines CI/CD y gestores de incidencias.

Un primer paso práctico

Elige una familia de productos. Mapea el responsable, la decisión de ámbito, la SBOM, el flujo de vulnerabilidades, las brechas del expediente técnico y la evidencia de release. Así el equipo obtiene una línea base CRA concreta sin convertir el cumplimiento en un proyecto separado.

Explora qué cubre CRA Evidence para tu producto en craevidence.com/es. Las opciones de precios y planes están disponibles en craevidence.com/es/precios.