SE

EMBEDDED SYSTEMS ENGINEERING

SCHMITT CONSULTING S.A.R.L. · SC-SARL.COM

Chequeo rápido CRA para fabricantes de dispositivos

La nueva ley de la UE sobre la ciberseguridad de los productos conectados — lo que debe estar listo antes de septiembre de 2026, en lenguaje claro.

Primer plazo vinculante: 11 de septiembre de 2026

No en 2027. Quien no se prepare ahora se quedará sin tiempo.

1 De qué se trata

El **Cyber Resilience Act** — en breve **CRA** — está en vigor desde diciembre de 2024. Establece qué grado de seguridad deben tener los productos conectados frente a los ataques procedentes de internet. Afecta a todo lo que contiene software o se conecta a una red: desde el termostato inteligente hasta los autómatas industriales y la aplicación.

Muchos fabricantes creen que tienen hasta finales de 2027. Eso solo es cierto para una parte de las obligaciones. El **primer plazo vinculante llega ya en septiembre de 2026** — y afecta también a productos que llevan tiempo en el mercado y aún reciben mantenimiento.

11 de septiembre de 2026

Obligación de notificación. Si una vulnerabilidad es explotada de forma demostrable por atacantes, debe notificarse a las autoridades **en un plazo de 24 horas**.

11 de diciembre de 2027

Todas las demás obligaciones. Producto seguro desde el diseño, actualizaciones de seguridad durante toda su vida útil, lista de materiales de software completa, evaluación formal y marcado CE.

Las posibles multas alcanzan hasta **15 millones de euros o el 2,5 % de la facturación anual mundial** — la cifra que sea mayor. Y: la ley se aplica expresamente también a pequeños fabricantes y proveedores individuales, no solo a las grandes corporaciones.

2 Los conceptos clave — explicados en breve

Firmware
El software de control integrado de forma permanente en un dispositivo y que hace que funcione — por ejemplo, el código de programa de una máquina, un sensor o un autómata.

Vulnerabilidad (fallo de seguridad)
Un error o una debilidad del software a través del cual un atacante puede penetrar en el dispositivo o manipularlo.

Lista de materiales de software (SBOM)
Una lista completa de todos los componentes de software de un producto — comparable a la lista de piezas de un componente, pero para el código de programa. Sin ella no se puede saber si el producto está afectado por una vulnerabilidad conocida.

ENISA / CSIRT
ENISA es la agencia de ciberseguridad de la UE, el organismo central de la seguridad informática en Europa. Los CSIRT son los «bomberos informáticos» nacionales que coordinan en caso de incidentes. A ellos va la notificación de 24 horas.

Seguridad funcional
La protección de un dispositivo frente a *fallos y averías* técnicas — práctica consolidada, por ejemplo, en la automoción. El CRA le añade la protección frente a *ataques intencionados*.

Marcado CE
El conocido marcado CE en los productos. Confirma que un producto cumple los requisitos de la UE y puede venderse en el mercado europeo.

3 ¿Está preparado para el CRA? La lista de verificación

Revise los siguientes puntos. Cada casilla que **no** pueda marcar con la conciencia tranquila es una tarea pendiente hasta septiembre de 2026.

VISIÓN GENERAL Y ORGANIZACIÓN

- ☐ Sabemos cuáles de nuestros productos están sujetos a la ley.
- ☐ Sabemos qué productos antiguos seguimos manteniendo (y que, por tanto, también están afectados).
- ☐ Existe una persona responsable del tema CRA en la empresa.

LISTA DE MATERIALES DE SOFTWARE

- ☐ Para cada producto existe una lista completa de todos los componentes de software integrados.
- ☐ En ella reconocemos también los componentes obsoletos que el proveedor ya no mantiene.
- ☐ Esta lista se mantiene actualizada de forma continua, no se crea una sola vez.

PROCESO DE NOTIFICACIÓN (OBLIGATORIO DESDE 09/2026)

- ☐ Está definido quién detecta una vulnerabilidad explotada.
- ☐ Está definido quién la evalúa y quién la notifica.
- ☐ Podemos cumplir realmente el plazo de 24 horas a nivel organizativo — también en fin de semana.

PROTECCIÓN TÉCNICA DEL DISPOSITIVO

- ☐ El software del dispositivo se almacena cifrado y no puede leerse sin más.
- ☐ Las actualizaciones son a prueba de manipulación — nadie puede inyectar software introducido de forma fraudulenta.
- ☐ El dispositivo puede recibir actualizaciones de seguridad durante toda su vida útil.
- ☐ Al arrancar, el dispositivo comprueba que solo se ejecuta software auténtico y sin alterar.

PRUEBAS Y DOCUMENTACIÓN

- ☐ Podemos demostrar que el desarrollo siguió normas de programación reconocidas.
- ☐ La fiabilidad y la resistencia a los ataques se piensan en un concepto común, no por separado.
- ☐ Los documentos necesarios para la posterior evaluación de conformidad se llevan desde el principio.

4 Cómo seguir

Los próximos meses decidirán si en septiembre de 2026 hay un proceso ordenado o si habrá que improvisar a toda prisa. Quien empieza pronto reparte el trabajo — y evita correcciones caras justo antes del plazo. La mayor palanca no suele estar solo en la técnica, sino en la buena articulación entre la lista de materiales, el proceso de notificación y la protección del dispositivo.

→ Profundizar y apoyo

¿No quiere solo entender los requisitos, sino implementarlos? Tres vías:

Libros técnicos y software

Conocimiento práctico de más de 35 años de desarrollo embebido — la base técnica detrás de los requisitos del CRA. Disponible en **sc-sarl.com/es/produkte.html**

De regalo: «Compendio de fórmulas para informáticos e ingenieros»

Compendio de fórmulas HTML interactivo, 56 capítulos, bilingüe DE/EN, utilizable sin conexión — gratis en el área de descargas.

Apoyo personalizado

Desde la lista de materiales de software hasta el endurecimiento del firmware. Consulta en **sc-sarl.com/es/kontakt.html**

A los productos y descargas →

Esta guía ofrece una visión práctica y no sustituye al asesoramiento jurídico. El texto de referencia es el Reglamento (UE) 2024/2847. Estado de los plazos: obligación de notificación desde el 11/09/2026, plena aplicabilidad desde el 11/12/2027.