Ferrita

El CRA para fabricantes con firmware.

Qué pide el Reglamento de Ciberresiliencia de la UE a vuestro producto y a vuestra empresa, con fechas, y qué hacer este trimestre.

Ferrita · ferritasec.com · Noviembre de 2026
Guía orientativa. No es asesoramiento jurídico.

Qué es y a quién afecta

El Reglamento (UE) 2024/2847, de Ciberresiliencia (CRA), hace responsable al fabricante de la seguridad de su producto durante toda su vida útil. Afecta a todo producto con elementos digitales que se venda en la UE: el software y el hardware con firmware que se conecta, directa o indirectamente, a otro dispositivo o a una red.

Quedan fuera, porque tienen su propia norma, los productos sanitarios, los vehículos homologados, la aviación, los equipos marinos y lo de uso exclusivo militar.

Las fechas

Fecha	Qué pasa
11-09-2026	**Ya en vigor.** Hay que avisar de las vulnerabilidades explotadas y de los incidentes graves que afecten a vuestros productos, también los ya vendidos.
Hoy	Las normas armonizadas del CRA aún no están publicadas. Un producto de clase I no puede autoevaluarse sin ellas: necesita un organismo notificado.
11-12-2027	Todo lo que se ponga en el mercado desde ese día cumple el CRA entero, **aunque sea el mismo modelo** que ya vendíais. Sin eso no hay marcado CE.

¿En qué clase está vuestro producto?

Clase	Ejemplos	Cómo se evalúa
Por defecto	La mayoría: sensores, pasarelas, maquinaria conectada, instrumentos	Autoevaluación del fabricante
Importante, clase I	Routers, módems y switches; productos de hogar inteligente con funciones de seguridad (cerraduras, cámaras, alarmas); sistemas operativos; productos con VPN	Autoevaluación solo aplicando íntegramente normas armonizadas o certificación. Hoy, organismo notificado
Importante, clase II	Cortafuegos, sistemas de detección y prevención de intrusiones, hipervisores, microcontroladores resistentes a manipulación	Organismo notificado
Crítico	Pasarelas de contador inteligente, dispositivos con caja de seguridad, tarjetas inteligentes	Organismo notificado o certificación europea

Resumen de los Anexos III y IV. La clase depende de la función principal del producto: hay que analizarla caso a caso.

Qué pide al producto

- Salir al mercado **sin vulnerabilidades explotables conocidas**.
- **Seguro por defecto:** sin credenciales comunes, con lo innecesario cerrado y con la opción de volver al estado de fábrica.
- Protección del acceso, de la confidencialidad y de la integridad de datos, firmware y configuración.
- **Actualizaciones de seguridad**, a ser posible automáticas, y separadas de las de funcionalidad cuando se pueda.
- Superficie de ataque mínima y registro de la actividad relevante para la seguridad.

Qué pide a vuestra empresa

- Un **SBOM** en formato estándar y legible por máquina, que cubra al menos las dependencias de primer nivel.
- Gestionar las vulnerabilidades durante el **periodo de soporte**, que como norma general es de al menos cinco años, con actualizaciones de seguridad gratuitas.
- Una **política de divulgación coordinada** y una dirección pública para que os comuniquen fallos.
- Una **evaluación de riesgos** y la **documentación técnica**, que se guarda diez años o lo que dure el soporte, si es más.
- La **declaración UE de conformidad** y el marcado CE.

El aviso: 24 horas, 72 horas, 14 días

Plazo	Vulnerabilidad explotada	Incidente grave
24 h	Alerta temprana	Alerta temprana
72 h	Notificación con detalle y medidas	Notificación con detalle y medidas
Final	Informe a los 14 días de tener la corrección	Informe al mes de la notificación

Se avisa por la plataforma única de ENISA, que lo hace llegar al CSIRT nacional. También hay que informar a los usuarios afectados y de cómo protegerse. La hora empieza a contar cuando lo sabéis, no cuando lo habéis analizado.

Las multas

Hasta **15 millones de euros o el 2,5 %** de la facturación mundial, lo que sea mayor, por incumplir los requisitos esenciales o las obligaciones de vulnerabilidades. Hasta 10 millones o el 2 % por otras obligaciones, y hasta 5 millones o el 1 % por dar información incorrecta a las autoridades.

Qué hacer este trimestre

- [ ] Hacer la lista de productos que vendéis en la UE y decidir la clase de cada uno, por escrito.
- [ ] Si alguno es clase I o superior, pedir hueco a un organismo notificado.
- [ ] Decidir quién recibe, decide y envía un aviso de 24 horas, también en vacaciones.
- [ ] Publicar una dirección para que os comuniquen vulnerabilidades (por ejemplo, un security.txt en vuestra web).
- [ ] Sacar el SBOM de la imagen que sale de fábrica de cada producto, no del repositorio.
- [ ] Revisar las vulnerabilidades que marca el escáner y separar las que de verdad se alcanzan, con la justificación escrita.
- [ ] Comprobar que las actualizaciones van firmadas y se pueden instalar en campo.
- [ ] Fijar el periodo de soporte de cada producto y cómo vais a cubrirlo.

Si queréis ayuda con cualquiera de estos pasos, empezamos con una llamada de 30 minutos sin coste y os mandamos por escrito qué os toca y qué es lo más urgente.

contact@ferritasec.com · +34 644 48 71 00 · ferritasec.com

Esta guía resume el Reglamento (UE) 2024/2847 para fabricantes. Es orientativa y no sustituye al texto del reglamento ni al asesoramiento jurídico. Revisada en noviembre de 2026.