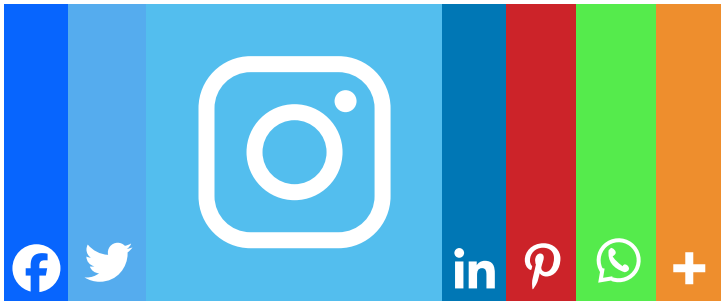
Spread the love



El Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.° 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia, CRA por sus siglas en inglés) introduce un sistema escalonado de verificación de conformidad, para que los productos con elementos digitales cumplen con estándares de ciberseguridad antes de su comercialización en la UE. La combinación de la **declaración de conformidad**, la **certificación** y el **marcado CE** refuerza la seguridad en el ecosistema digital europeo

1. Declaración UE de Conformidad (Artículo 20 CRA)

Es un documento obligatorio que el fabricante debe emitir para confirmar que su producto cumple con los requisitos esenciales de ciberseguridad establecidos en el **Anexo I** del Reglamento.

- Es exigida para **todos los productos con elementos digitales** que entran en el mercado de la UE.
- Permite la **libre circulación** de estos productos dentro del mercado único europeo.
- Debe mantenerse **actualizada y accesible** para las autoridades nacionales competentes durante al menos 10 años después de que el producto haya sido comercializado.
- Su contenido mínimo está detallado en el **Anexo V** del Reglamento.

2. Certificación Europea de Ciberseguridad (Artículo 21 CRA)
Para productos considerados de mayor riesgo, el Reglamento exige una **certificación de ciberseguridad** que verifique su conformidad con los estándares europeos.

- Aplica a los **productos críticos con elementos digitales** enumerados en el **Anexo IV** del CRA.
- La certificación se realiza bajo esquemas europeos de certificación regulados por el **Reglamento (UE) 2019/881** sobre ciberseguridad.
- Existen **tres niveles de garantía**, en función del riesgo:
  - **Básico**: Protección contra riesgos mínimos.
  - **Sustancial**: Protección frente a ataques más sofisticados.
  - **Alto**: Garantiza un alto nivel de resistencia ante amenazas avanzadas.
- La certificación debe ser realizada por **Organismos de Evaluación de la Conformidad**, acreditados por los Estados miembros y supervisados por la Agencia de la Unión Europea para la Ciberseguridad (**ENISA**).

3. Marcado CE y Obligaciones del Fabricante (Artículos 18 y 19 CRA)
El **marcado CE** indica que un producto cumple con los requisitos del CRA y que puede comercializarse en la UE.

- Con el marcado, el fabricante garantiza que el producto ha pasado los procedimientos de evaluación de conformidad.
- Debe ser **visible, legible e indeleble** en el propio producto, su embalaje o su documentación.
- Las autoridades nacionales pueden solicitar pruebas de conformidad y, en caso de incumplimiento, exigir la retirada del producto del mercado.

4. Procedimientos de Evaluación de la Conformidad (Artículo 22 CRA)
El CRA establece diferentes procedimientos para evaluar si un producto cumple con los requisitos de ciberseguridad:

i. **Control interno de la producción**:

   - Aplicable a productos con menor impacto en la ciberseguridad.
   - El fabricante realiza una **autoevaluación** y emite la Declaración UE de Conformidad.

ii. **Gestión de calidad total**:

   - Aplicable a productos con **mayor impacto en la ciberseguridad** (por ejemplo, los del **Anexo III** del Reglamento).
   - Requiere que un **organismo independiente supervise el sistema de gestión** de calidad del fabricante.

iii. **Evaluación por un organismo notificado**:

   - Obligatorio para **productos críticos** incluidos en el **Anexo IV**.
   - Un o**rganismo de certificación independiente** (acreditado para certificar) verifica la conformidad antes de su comercialización.