

CRA

¿QUÉ ES?

El Cyber Resilience Act (CRA) es una norma europea que establece requisitos de ciberseguridad para los productos con elementos digitales que se comercializan en la Unión Europea.

Su objetivo es que estos productos sean seguros desde el diseño y durante todo su ciclo de vida, obligando a tener en cuenta los riesgos, gestionar vulnerabilidades y mantener actualizaciones de seguridad cuando sea necesario.

¿De dónde viene?

El CRA surge como respuesta al aumento de productos conectados y de las vulnerabilidades en software y hardware. La Unión Europea lo aprobó en 2024 para establecer unas reglas comunes de ciberseguridad y reforzar la protección de los productos digitales durante todo su ciclo de vida.



El CRA cambia la forma de entender la ciberseguridad de los productos digitales: la seguridad debe garantizarse desde su diseño y mantenerse también después de su comercialización.

¿CÓMO FUNCIONA EL CRA?

Si una empresa **fabrica o comercializa un producto con elementos digitales**, tendrá que garantizar que cumple unos requisitos mínimos de ciberseguridad antes de ponerlo en el mercado.

La responsabilidad no termina con la venta. Durante el periodo de soporte del producto, la empresa deberá vigilar posibles vulnerabilidades, **corregir fallos de seguridad y publicar actualizaciones o parches cuando sea necesario**.

Esto significa que, si aparece un problema de ciberseguridad relacionado con ese producto, el fabricante deberá **actuar para solucionarlo y reducir el riesgo**, no solo cuando ya ha ocurrido un incidente sino también de forma preventiva.

CRA

¿POR QUÉ SE CREA Y QUÉ QUIERE CONSEGUIR EL CRA?

1. Más productos conectados, más riesgos

El aumento de software, hardware y dispositivos conectados ha incrementado también las vulnerabilidades.

Objetivo: Conseguir productos más seguros desde el diseño

2. Vulnerabilidades que no siempre se corrigen a tiempo

Muchos productos siguen en uso aunque aparezcan fallos de seguridad.

Objetivo: Garantizar actualizaciones y correcciones durante el periodo de soporte.

3. Falta de responsabilidad después de la venta

Hasta ahora no siempre estaba claro quién debía responder por la seguridad del producto una vez comercializado.

Objetivo: Aumentar la responsabilidad de los fabricantes durante todo el ciclo de vida.

4. Diferencias entre productos y países

No existía un marco único que estableciera las mismas exigencias de ciberseguridad en toda la UE.

Objetivo: Crear unas reglas comunes para los productos con elementos digitales.

5. Dificultad para saber si un producto es seguro

Los usuarios y empresas no siempre disponen de información suficiente sobre su nivel de seguridad.

Objetivo: Aumentar la transparencia y la confianza en los productos digitales.

“Los productos con elementos digitales se diseñarán, desarrollarán y producirán de manera que garanticen un nivel adecuado de ciberseguridad sobre la base de los riesgos existentes.”

Reglamento (UE) 2024/2847 – Cyber Resilience Act.

“El incumplimiento del CRA puede conllevar sanciones importantes y, en determinados casos, multas de hasta 15 millones de euros o el 2,5 % de la facturación anual mundial de la empresa.”

Reglamento (UE) 2024/2847 – Cyber Resilience Act, art. 64.2

CRA

¿TIENE MI EMPRESA QUE CUMPLIR CRA?

☐ **¿Fabricamos o desarrollamos productos con elementos digitales?**

Software, hardware, equipos conectados o componentes digitales

☐ **¿Vendemos o comercializamos esos productos en la Unión Europea?**

El CRA se aplica a los productos con elementos digitales que se ponen en el mercado europeo.

☐ **¿Importamos productos digitales fabricados fuera de la UE?**

Los importadores también tienen obligaciones de comprobación.

☐ **¿Distribuimos o vendemos productos digitales de otros fabricantes?**

Los distribuidores deben verificar que el producto cumple determinados requisitos antes de comercializarlo.

☐ **¿Modificamos de forma importante un producto digital y después lo vendemos?**

En algunos casos, una modificación sustancial puede hacer que la empresa pase a asumir obligaciones de fabricante.

Si el CRA aplica a tu empresa, ¿Qué tienes que hacer?

Primero identifica qué papel tiene tu empresa en la cadena de comercialización del producto

DISTRIBUIDOR

- Comprobar que el producto incluye el marcado y la documentación exigida
- Verificar que fabricante e importador han cumplido sus obligaciones
- No vender productos cuando existan indicios de incumplimiento

IMPORTADOR

- Comprobar que el fabricante ha cumplido con los requisitos del CRA
- Verificar la documentación y el marcado CE
- Asegurarse de que el producto puede comercializarse en la UE
- No introducir en el mercado productos que no sean conformes

FABRICANTE

- Diseñar el producto teniendo en cuenta la ciberseguridad
- Evaluar los riesgos antes de comercializarlo
- Gestionar vulnerabilidades durante el periodo de soporte
- Publicar actualizaciones y parches cuando sea necesario
- Preparar la documentación técnica y demostrar la conformidad
- Notificar vulnerabilidades e incidentes graves cuando corresponda