Cyber Resilience Act (CRA) de la Unión Europea

"En un mundo donde todo está conectado, la ciberseguridad es la base de la confianza digital."

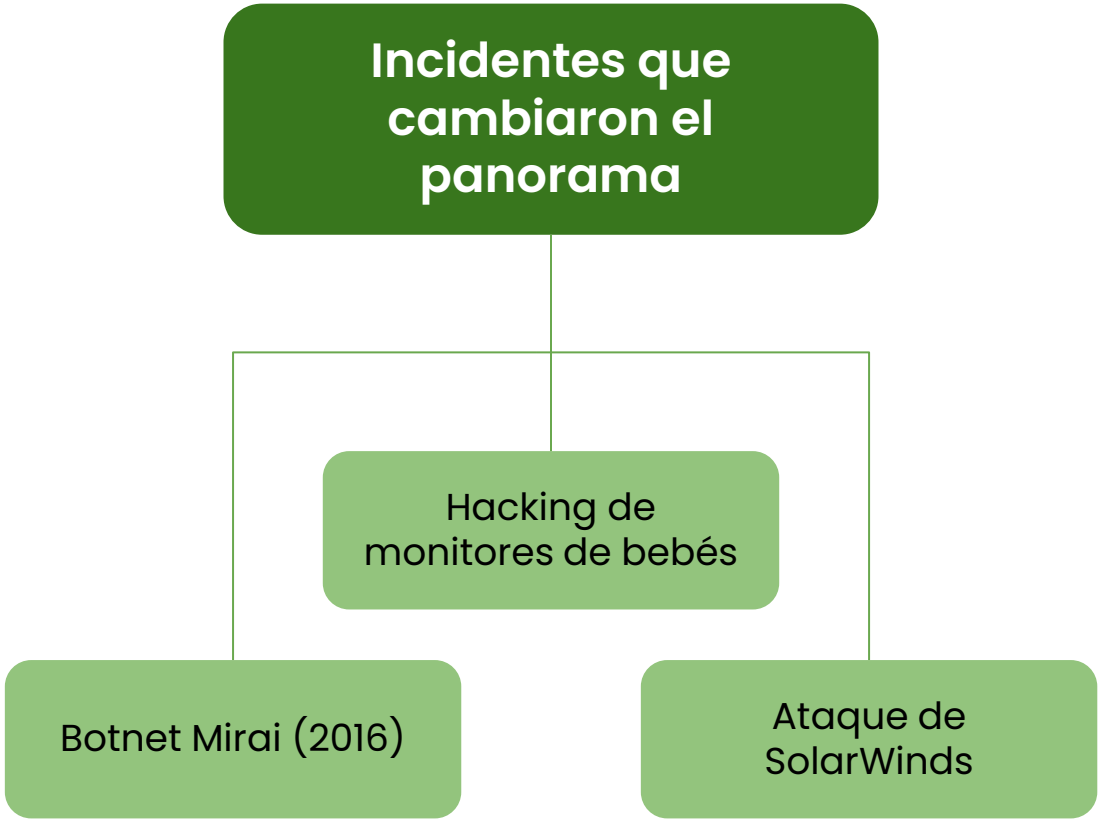
Introducción.
La nueva era digital.

Imaginen una tienda de barrio en 2024: no solo tiene una persiana metálica, sino también sistemas de pago digital, cámaras IoT y gestión de inventario en la nube. Cada uno de estos elementos es una puerta digital que necesita protección.

El Cyber Resilience Act es el Reglamento (UE) 2024/2847, la primera legislación europea que establece requisitos obligatorios de ciberseguridad para productos con elementos digitales.

Dato clave: El 60% de las pymes afectadas por ciberataques cierran en 6 meses (fuente: UE).

Contexto del CRA.
¿Por qué surge el CRA?.



Alcance y cronograma.
¿Qué cubre el CRA y cuándo aplica?

Obligaciones

La ciberseguridad debe estar integrada desde el diseño inicial hasta su retirada del mercado, y es responsabilidad de fabricantes, importadores y distribuidores.

Cronograma de implementación gradual

10 de diciembre de 2024
Entrada en vigor del reglamento

11 de junio de 2026
Obligaciones para organismos notificados

11 de septiembre de 2026
Obligación de notificar vulnerabilidades e incidentes en 24 horas

11 de diciembre de 2027
Cumplimiento pleno de todos los requisitos

Semáforo de riesgo. Categorización proporcional.

Principio de proporcionalidad

- **Categoría por defecto (Luz Verde) - 90% del mercado**
- **Productos importantes (Luz Ámbar) - Clases I y II**
- **Productos críticos (Luz Roja) - Máxima exigencia**

Ejemplo

Un termostato inteligente (verde) vs. un marcapasos conectado (rojo): requisitos muy distintos

Proceso de reclasificación

Si un producto sufre un ataque grave, puede pasar a categoría superior

Pilares para proveedores. Obligaciones clave.

Evaluación de riesgos previa

Antes de lanzar un producto, deben identificar amenazas, vulnerabilidades y posibles impactos

Seguridad por diseño y por defecto

Incluir desde el inicio medidas como contraseñas seguras, cifrado, separación de privilegios y configuración segura predeterminada

Gestión de vulnerabilidades durante 5 años

Proveer actualizaciones gratuitas, monitorear fallos, aplicar parches automáticos y mantener comunicación con los usuarios

Documentación técnica

Mantener un registro completo (SBOM, riesgos, medidas, procesos) accesible para las autoridades durante 10 años

Notificación de incidentes

Desde septiembre de 2026, informar vulnerabilidades explotadas en 24 horas y presentar un informe completo en 72 horas, además de alertar a los usuarios afectados

Beneficios para consumidores y empresas.

Para los consumidores

- Marcado CE de ciberseguridad
- Actualizaciones gratuitas garantizadas
- Información transparente

Para las empresas usuarias

- Reducción del riesgo
- Decisiones de compra informadas
- Reducción de costes de incidentes

Para los fabricantes pioneros

- Acceso garantizado al mercado europeo
- Diferenciación competitiva
- Reconocimiento internacional

Sanciones.
Coste por incumplimiento.

- **Elevadas multas**
- **Daño reputacional**
- **Medidas adicionales**
  - Retirada inmediata del mercado
  - Prohibición temporal de comercialización
  - Auditorías exhaustivas

Hoja de ruta de cumplimiento.

Paso 1: Inventario digital exhaustivo

Paso 2: Clasificación según el semáforo de riesgo

Paso 3: Plan de seguridad por diseño

Paso 4: Sistema de gestión de vulnerabilidades

Paso 5: Capacitación y cultura organizacional

Cierre.
Puntos clave.

Necesidad urgente

Los productos inseguros ya no son aceptables en una sociedad interconectada

Alcance universal

Se aplica a casi todo lo que se conecta, desde juguetes hasta infraestructuras críticas

Sistema proporcional

Establece categorías de riesgo y obligaciones escalonadas según la criticidad

Beneficia a todos

Consumidores protegidos, empresas más seguras, fabricantes con ventaja competitiva

Sanciones importantes

Las multas de hasta 15 millones de euros y el plazo de preparación limitado exigen acción inmediata

Cierre.
Los grades retos del futuro.

Pregunta 1	¿Cómo convivirá el CRA con normas sectoriales como DORA o NIS2?
Pregunta 2	¿Podrá la industria soportar el coste de auditorías externas?
Pregunta 3	¿Veremos un "nutri-score" de ciberseguridad visible en la caja del producto?

Gracias por su atención