La ley de Ciberresiliencia

Ciberresilencia

La Ley de Ciberresiliencia (CRA) es la primera legislación de la UE que establece requisitos obligatorios de ciberseguridad para los productos que incluyen elementos digitales.

Entró en vigor el 10 de diciembre de 2024 y tiene un plazo de 3 años para adaptación.

¿Qué es la ciberresilencia?

La ciberresiliencia se refiere a la capacidad de una organización o sistema para anticipar, resistir, recuperarse y adaptarse ante incidentes cibernéticos, garantizando la continuidad y seguridad de sus operaciones.

Un mundo interconectado

Cámaras de bebés, relojes, neveras, peceras, coches, marcapasos, roombas.

Actualmente los objetos menos pensados tienen conexión a internet y pueden ser susceptibles a vulnerabilidades y ciberataques

Ciberataque

Es un intento maligno de acceder, dañar o interrumpir sistemas informáticos, redes, dispositivos o datos sin autorización.

¿A quién afecta?

La ley afecta a fabricantes, distribuidores e importadores de productos con elementos digitales que deseen comercializar sus productos en el mercado europeo.

¿Qué es la ciberresilencia?

La Ley de Ciberresiliencia de la Unión Europea, tiene como objetivo proteger a consumidores y empresas de amenazas cibernéticas, asegurando que los productos de hardware y software sean más seguros. Para ello establece responsabilidades, obligaciones y sanciones

Obligaciones principales

Evaluación de riesgos: Identificar y documentar posibles vulnerabilidades.
Implementación de medidas de seguridad: Aplicar controles técnicos y organizativos para mitigar riesgos.
Actualizaciones y soporte: Proporcionar actualizaciones de seguridad durante el ciclo de vida del producto.
Transparencia: Informar sobre la seguridad del producto y cualquier posible riesgo asociado

Soy una PYME ¿Qué hago?

Las obligaciones afectan a todas las empresas, incluídas las PYMES.

Según una encuesta realizada por ENISA los incidentes de ciberseguridad suponen un impacto negativo grave que no pueden asumir.

El **57 %** dice que podría llegar a cerrar o quedar en bancarrota a la semana de recibir el ciberataque.

Para preparse lo primero es:

1. Formación y concienciación.
2. Evaluación de productos.
3. Implementación de procesos.
4. Documentación.

akme!

Software libre

Se llama software libre a todo el software que permita el uso, estudio modificación y distribución sin restricciones.

¿Le afecta la CRA?

✓ El software libre se verá afectado si se comercializa integra o usa en productos digitales.

✗ Si el software libre es desarrollado y distribuido de manera no comercial no está sujeto a la ley

Con un ejemplo

No aplica la ley: Un programador independiente contribuye a un proyecto de código abierto en GitHub sin fines de lucro.

Eso significa...

Esto significa que las empresas que integran software libre en productos comerciales sí deben cumplir con la normativa.

Soy una PYME ¿Qué hago?

Revisar qué software libre está integrado en el producto.

- Verificar si hay vulnerabilidades conocidas en bases de datos o en la información del proyecto.
- Evaluar si el software sigue siendo mantenido, recuerda que si no recibe actualizaciones, puede ser un riesgo.
- Mantente al día con las actualizaciones y parches de seguridad que pueda aportar la comunidad y, en caso de detectarlo y solucionarlo ¡comparte!
- Crea un protocolo o plan de respuesta a incidentes, así asegurarás los deberes de información y transparencia para tus consumidores y usuarios.

Sanciones

Las empresas que no cumplan pueden enfrentar multas de hasta 15 millones de euros o el 2,5 % de su facturación anual mundial, lo que sea mayor.

akme!