



BOLETÍN SEMANAL DEL MCCE

Del 09/10 al 16/10 de 2026



España acumula un retraso prolongado en la transposición de la Directiva NIS2 y compromete su resiliencia digital

El lento avance legislativo para incorporar la Directiva NIS2 al ordenamiento jurídico nacional mantiene a España en una situación de vulnerabilidad e incertidumbre regulatoria frente a los ciberataques. Esta falta de transposición dentro de los plazos fijados por la Unión Europea expone al país a posibles expedientes de infracción y sanciones económicas por parte de las instituciones comunitarias.

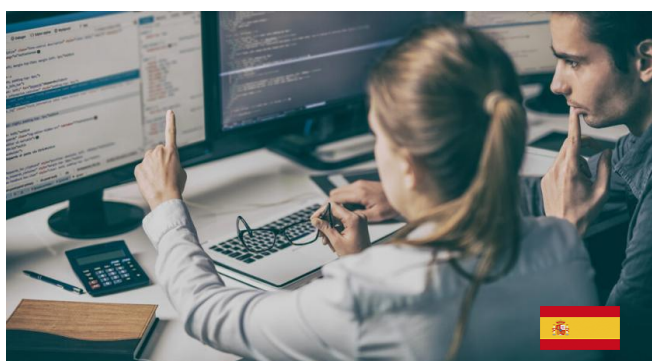
[+ Más información](#)



Récord en 2025 con más de 120.000 ciberataques gestionados por INCIBE

El INCIBE gestionó una cifra récord de incidentes durante el pasado año y los ataques semanales a las empresas españolas se dispararon este verano. La alta sofisticación de las amenazas actuales y la dependencia tecnológica agravan la vulnerabilidad del tejido empresarial.

[+ Más información](#)



La escasez de personal frena la defensa frente a ciberataques con IA

El informe anual de ISACA advierte sobre un incremento notable de los ciberataques y una persistente falta de recursos en los equipos de defensa. Las organizaciones afrontan una brecha severa de personal capacitado y un crecimiento constante del estrés operativo entre sus especialistas.

[+ Más información](#)



BOLETÍN SEMANAL DEL MCCE

Del 09/10 al 16/10 de 2026



Europa reclama controles más estrictos ante el riesgo de ciberataques a la fotovoltaica

La creciente digitalización de la energía solar genera nuevos riesgos para la estabilidad del suministro eléctrico. Los atacantes pueden explotar fallos en los inversores para provocar desequilibrios graves en la red. Bruselas pide endurecer los controles normativos.

[+ Más información](#)



Ciberataque arruina alimentos frescos y congelados en supermercados franceses

Un ataque informático contra sistemas de refrigeración de varios supermercados en Francia destruyó numerosas mercancías perecederas. Este sabotaje tecnológico provocó daños económicos graves en cadenas comerciales del país.

[+ Más información](#)

Otras noticias



El aprendizaje automático transforma el análisis en ciberseguridad

La integración del machine learning permite correlacionar millones de eventos diarios y detectar anomalías complejas en la red. Estos modelos identifican variaciones en los patrones habituales de tráfico antes de la catalogación oficial de la amenaza.

[+ Más información](#)



La IA ofensiva eleva la ciberseguridad a la dirección estratégica

El auge de la inteligencia artificial utilizada por cibercriminales exige situar la ciberprotección en el centro de las decisiones corporativas. Las ciberamenazas automatizadas obligan a los órganos directivos a supervisar la resiliencia operativa y la inversión defensiva de forma continua.

[+ Más información](#)