WEEKLY BULLETIN OF THE MCCE

From 9 to 16 October 2026



Spain accumulates a prolonged delay in the transposition of the NIS2 Directive and compromises its digital resilience

The slow legislative progress to incorporate the NIS2 Directive into the national legal order keeps Spain in a situation of vulnerability and regulatory uncertainty in the face of cyberattacks. This lack of transposition within the deadlines set by the European Union exposes the country to possible infringement proceedings and economic sanctions by the EU institutions.

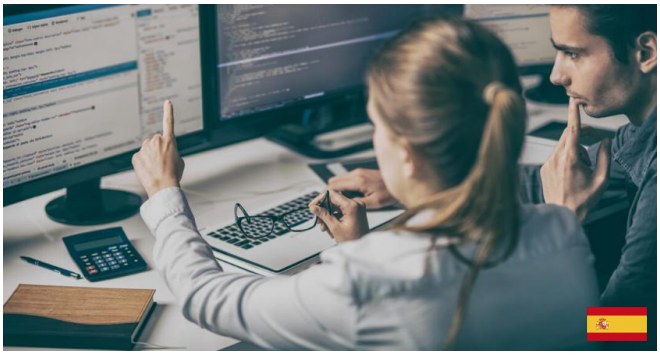
+ More information



Record in 2025 with more than 120,000 cyberattacks managed by INCIBE

INCIBE managed a record number of incidents during the past year and weekly attacks on Spanish companies soared this summer. The high sophistication of current threats and technological dependence aggravate the vulnerability of the business fabric.

+ More information



Staff shortage slows defence against AI-powered cyberattacks

ISACA's annual report warns of a notable increase in cyberattacks and a persistent lack of resources in defence teams. Organisations face a severe gap in trained personnel and a constant growth in operational stress among their specialists.

+ More information

WEEKLY BULLETIN OF THE MCCE

From 9 to 16 October 2026



Europe calls for stricter controls against the risk of cyberattacks on photovoltaics

The growing digitalisation of solar energy generates new risks for the stability of the electricity supply. Attackers can exploit flaws in inverters to cause serious imbalances in the grid. Brussels calls for tightening regulatory controls.

+ More information



Cyberattack ruins fresh and frozen food in French supermarkets

A cyberattack against refrigeration systems of several supermarkets in France destroyed numerous perishable goods. This technological sabotage caused serious economic damage in commercial chains in the country.

+ More information

Other news

Machine learning transforms analysis in cybersecurity

The integration of machine learning makes it possible to correlate millions of daily events and detect complex anomalies in the network. These models identify variations in usual traffic patterns before the official cataloguing of the threat.

+ More information

Offensive AI elevates cybersecurity to strategic management

The rise of artificial intelligence used by cybercriminals requires placing cyber protection at the centre of corporate decisions. Automated cyber threats force governing bodies to continuously supervise operational resilience and defensive investment.

+ More information