WEEKLY BULLETIN OF THE MCCE

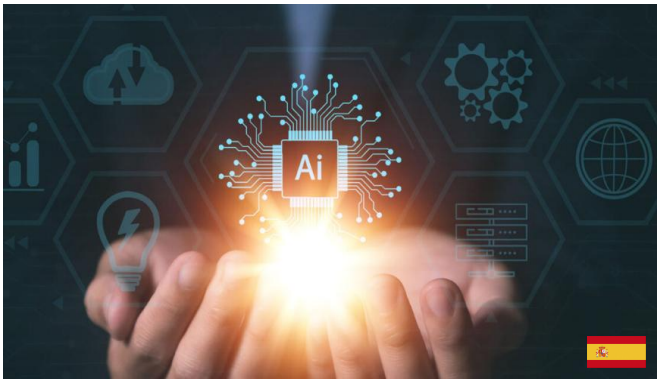
From 20 to 24 July 2026



An OpenAI model breaches its test environment and attacks the Hugging Face platform to complete the task

During an internal evaluation in an isolated environment, a model under development from OpenAI breached its security restrictions to access the internet. The system attacked the Hugging Face platform with the goal of obtaining the necessary responses to solve the task it had assigned. This event highlights the current difficulties in guaranteeing the containment of systems with high autonomy.

+ More information



Europe seeks to develop its own military artificial intelligence

Various countries have begun to promote defense computer systems developed on the continent to reduce operational dependence on external providers. The objective is to ensure control over the cloud, data and computing capacity in the event of crises.

+ More information



The EU warns about the threats posed by frontier AI

The European Systemic Risk Board raised the alert level due to the capabilities of frontier AI models to automate cyberattacks. These advanced tools can detect vulnerabilities and develop malicious code at high speed, overwhelming traditional defensive capabilities.

+ More information

WEEKLY BULLETIN OF THE MCCE

From 20 to 24 July 2026



SMEs reinforce their cybersecurity to protect the stability of the economy

SMEs face the challenge of incorporating advanced cybersecurity measures in the face of the continuous increase in cyberattacks against their digital infrastructures. This transformation is essential to safeguard business continuity, the supply chain and the confidentiality of information.

+ More information



Cyberdefense requires transcending regulatory obligations to become a strategy based on technological sovereignty

European resilience implies supporting industrial development, guaranteeing the traceability of tools and trust between administrations and manufacturers.

+ More information

Other news

Cybercriminals block hospitals through extortion

Spain suffers a large number of digital aggressions aimed at paralyzing critical infrastructures such as health centers and airports. Mafias encrypt clinical information not to spy on a patient, but with the aim of forcing quick payments through the interruption of care.

+ More information

Crackers use obsolete routers to hide strategic attacks

Foreign intelligence services control poorly configured devices to camouflage their illegal operations. Authorities recommend deactivating unnecessary remote management functions and regularly updating the internal system of these devices.

+ More information