WEEKLY BULLETIN OF THE MCCE

From 27 to 31 July 2026



Artificial intelligence transforms global digital security and triples its financial investment

Global cybersecurity enters an unprecedented stage driven by the development of artificial intelligence. Organizations will exponentially increase their digital protection budgets over the next five years to face advanced threats. In addition, this economic growth will require greater technical specialization and new defense strategies in all productive sectors.

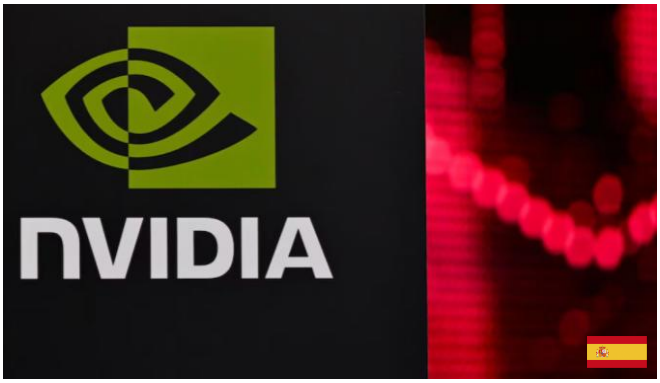
+ More information



Large tech companies promote open cyber tools

Nvidia leads a massive alliance together with thirty companies in the sector to reinforce security in artificial intelligence systems. The group develops open-source tools designed to detect vulnerabilities and protect models against cyberattacks.

+ More information



AI barriers hinder work in offensive cybersecurity

Cybersecurity experts and researchers point out that the controls imposed on artificial intelligence models hinder the detection of flaws and the creation of defenses. By blocking certain responses, the restrictions force some professionals to use open models executed locally.

+ More information

WEEKLY BULLETIN OF THE MCCE

From 27 to 31 July 2026



Cyberattacks via NFC on Android devices increase by 188%

The increase in cyberattacks using NFC technology puts the security of Android device users at risk. This modality takes advantage of contactless payment and transfer functions to compromise sensitive data and financial information.

+ More information



A group in Congress has presented a bill to require an emergency deactivation mechanism in the most advanced AI models

The initiative seeks to grant the Government the power to interrupt the functioning of these systems in the face of risks to public or national security.

+ More information

Other news

Cybercriminals intensify their attacks during the summer

The increase in electronic commerce during the summer multiplies cyber scams through identity theft techniques and fake portals. Attackers take advantage of the appeal of large discounts to obtain personal data or banking information from users. Strict verification of web domains and the use of secure payment gateways allow mitigating the impact of these threats.

+ More information

Companies integrate computer protection into their strategy

Computer security ceases to be a mere technical shield to become an essential factor of business growth. A global study indicates that organizations prioritize data protection, the secure adoption of new technologies and financial resilience.

+ More information