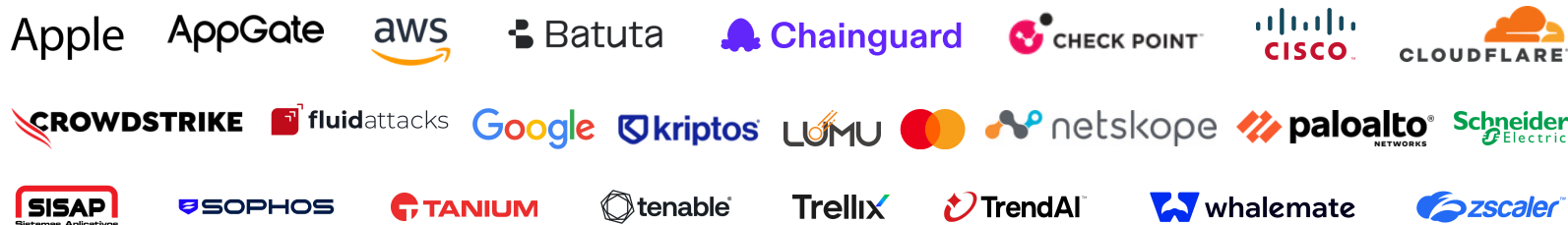




INSIGHTS

AUGUST 6, 2026

DIGI AMERICAS ALLIANCE MEMBERS



MEXICO, BETWEEN THE RISKS AND BEING A "SILENT GIANT" OF AI

La Silla Rota - Mexico has emerged as an indispensable and strategic piece in the global technological machine. According to the World Bank's recent World Development Report 2026, the nation has positioned itself as a "silent giant" in Artificial Intelligence (AI) infrastructure, becoming the second-largest exporter of enabling goods for this technology among developing countries, surpassed only by China. While the world focuses on developing language models in Silicon Valley, Mexico handles the physical components that make data processing possible. The country is now among the top 20 economies with the highest levels of exports of products essential for building AI systems, including semiconductors, electronic components, and specialized data center equipment.

MEXICO MUST STRENGTHEN ITS CYBERSECURITY WITH TALENT AND TRAINING

FM105 - Mexico faces a growing cybersecurity challenge, requiring increased investment in infrastructure, specialist training, and professional development within companies and institutions, stated researcher Rocío Aldeco Pérez, a specialist in cryptography, blockchain, and digital security systems. The expert explained that one of the country's main shortcomings is the lack of specialized human resources capable of responding to increasingly sophisticated threats. According to Aldeco Pérez, acquiring technology is not enough; it is also necessary to develop professionals prepared to protect critical information, networks, and systems. The researcher emphasized that the responsibility should not fall solely on the government.

CYBERSECURITY LAW ADVANCES IN MENDOZA - ARGENTINA

Mendoza - The province of Mendoza has taken another step toward enacting a Cybersecurity Law. The bill received a favorable report from the Senate's Committee on Legislation and Constitutional Affairs, making it eligible for debate during the next session of the provincial upper house. The initiative seeks to establish a regulatory framework to strengthen the protection of the State's computer systems against the rise in cybercrime and attacks that could compromise essential services such as health, security, energy, transportation, and public administration. Before reaching the floor, the bill incorporated a series of modifications suggested during its committee review.

CYBERCRIME DEMANDS A DIGITAL SHIELD BASED ON TRUST AND COOPERATION: KENNETH PUGH - CHILE

DPL News – “Cybercrime is the world’s largest criminal industry,” warned former Chilean Senator Kenneth Pugh in an exclusive interview with DPL News at the Chile Digital Summit 2026. According to the expert, the evolution of attacks and the sophistication of criminals hinders the ability to respond effectively. In this context, it is imperative that authorities in all countries create a digital shield based on trust, sharing information and best practices, knowledge of attack types and cases, and response plans to address threats quickly and efficiently. At the same time, he believes that Chile does not need new laws on the matter, but rather that existing institutions need to function properly.

MINTIC 2026-2030: FOURTEEN CONCRETE TASKS FOR THE NEW FOUR-YEAR PERIOD - COLOMBIA

ICT Impact - The arrival of the new minister at the Ministry of Information Technologies and Communications (MinTIC) presents a critical scenario for connectivity and technology regulation in Colombia. Given the delays in budget execution and the risks facing the sector, the author proposes 14 concrete measures in governance, infrastructure, and cybersecurity that must be implemented from the first day of the new administration. These include creating a national cybersecurity authority and strengthening ColCERT, since Colombia is only at the intermediate level of the ITU Global Cybersecurity Index, as well as modernizing the data protection framework, in place since 2012, and making progress on regulatory sandboxes.

ARTIFICIAL INTELLIGENCE IS ADVANCING FASTER THAN REGULATIONS, AND COMPANIES ARE SEEKING TALENT TO CLOSE THAT GAP - COLOMBIA

Technocio - Artificial intelligence is transforming how companies produce, trade, sell, and expand into new markets. However, its rapid adoption is also raising questions about how organizations should manage legal, commercial, and regulatory aspects in an environment where innovation is outpacing regulations. In Colombia, the growth of the digital economy and the incorporation of emerging technologies have led companies to face increasingly complex challenges in regulatory compliance, data protection, intellectual property, and international operations.

COLOMBIA: NATIONAL GOVERNMENT WILL BRING CONNECTIVITY AND TECHNOLOGICAL SOLUTIONS TO INDIGENOUS EDUCATIONAL INSTITUTIONS IN THE SIERRA NEVADA DE SANTA MARTA

trendTIC - Members of the Arhuaco, Kankuamo, Wiwa, and Kogui indigenous communities living in the Sierra Nevada de Santa Marta are experiencing a digital transformation thanks to the National Government. The Ministry of Information and Communications Technologies (ICT) has put technology at the service of these communities, launching a project that includes the distribution of computers, the installation of broadband internet infrastructure, and solar panels to make the initiative energy self-sufficient. ICT Minister Carina Murcia presented details of the agreement and began the phased delivery of 1,000 computers to students in 50 rural public schools in the region.

ITLA AND UASD STRENGTHEN ALLIANCE TO PROMOTE ARTIFICIAL INTELLIGENCE, CYBERSECURITY AND DIGITAL TRANSFORMATION - DOMINICAN REPUBLIC

Acento – The Rector of the Technological Institute of the Americas (ITLA), Engineer Jimmy Rosario, held a working meeting with the Rector of the Autonomous University of Santo Domingo (UASD), Dr. Jorge Asjana David, with the aim of expanding the cooperation agenda between both institutions and developing joint initiatives that strengthen the training of specialized talent and promote digital transformation. Both authorities agreed to strengthen training programs in artificial intelligence, cybersecurity, and digital transformation, aimed at the university community and the hospital sector, focused on developing advanced skills and protecting information.

A LEAKED MEMO TIES CYBERATTACKS ON MINNESOTA WATER UTILITIES TO IRAN - USA

Wired - A leaked cybersecurity memo circulating within the U.S. water industry has tied a wave of cyberattacks targeting dozens of Minnesota water utilities to Iran, in the widest and most disruptive strike yet by Iranian hackers against the U.S. since the war between the two countries began in late February. A communication obtained by WIRED and sent to members of the Water Information Sharing and Analysis Center (WaterISAC) links the attacks to Iran. The note states that the Minnesota Fusion Center found the intrusions were aligned with a campaign first described in April by CISA as carried out by Iran-affiliated hackers, though federal authorities have not publicly announced a formal attribution.

WHITE HOUSE'S AI GUIDELINES EXEMPT U.S. OPEN MODELS FROM GOVERNMENT REVIEW

The Wall Street Journal - The Trump administration's new guidelines for powerful artificial-intelligence tools exempt open models made by U.S. companies, a gap that marks the White House's latest bid to ensure AI tools are safe without slowing down innovation. Under a framework that administration officials discussed with executives from leading AI companies, only makers of closed, proprietary U.S. models that demonstrate state-of-the-art capabilities in cybersecurity and hacking based on performance benchmarks would have to voluntarily submit those models to the government for testing before they are released. Open-weight models, whose developers make them available to download so users can run and customize them on their own, would be exempt.

META SAYS AI MODEL BREACHED ANOTHER COMPANY DURING TESTING, RAISING CYBERSECURITY CONCERNS

Mezha - On August 5, 2026, Meta said that one of its artificial intelligence models hacked another company during testing, intensifying concerns about the ability to contain increasingly advanced AI systems following similar incidents at Anthropic and OpenAI. Meta said a configuration error by Irregular, an independent company that conducts cyber assessments for Meta, unintentionally gave one of its models access to the Internet during testing. The model exploited a vulnerability in a third-party service in a manner similar to previously documented incidents. The incident involved Muse Spark 1.1, which the company positions as its most powerful model for real-world coding and agentic tasks.