DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 6, 2026

DIGI AMERICAS ALLIANCE MEMBERS

MEXICO RECONFIGURES ITS DATA GOVERNANCE AMID THE AI REGULATORY VACUUM

El Economista - Following the dissolution of the INAI (National Institute for Transparency, Access to Information and Personal Data Protection) and the transfer of its functions to the Executive branch, Mexico is discussing standards, audits, and impact assessments for high-risk AI systems in an environment where models already influence automated decisions without clear obligations of transparency or explanation. Data protection has entered a stage of institutional restructuring in Mexico as artificial intelligence is integrated into everyday work processes, with risks that intersect with privacy, security, identity, and trust in digital transactions, according to specialists who participated in the 1st International Forum on Personal Data Protection, organized by the Mexican Academy of Cybersecurity and Digital Law (AMCID).

WITH 10 SUBMARINE CABLES, COLOMBIA IS POSITIONING ITSELF AS A DIGITAL GATEWAY TO SOUTH AMERICA

La Nota Economica - Colombia currently has 10 submarine cables, representing a key strength for the development of the data center and data technology sector. This infrastructure enables high availability, redundancy, low latency, and greater resilience in communications—essential conditions for the operation of world-class data centers. Thanks to its geographic location and this network of submarine cables, Colombia is consolidating its position as a gateway to South America, efficiently connecting with North America, Central America, and other continents. This advantage not only facilitates large-scale data transit but also makes the country a strategic location for the installation of data centers seeking to serve regional and international markets.

NEW REGULATION ESTABLISHES QUANTUM CRYPTOGRAPHY IN GOV.BR AND DIGITAL CERTIFICATES - BRAZIL

FENATI - Quantum Cryptography – The National Institute of Information Technology (ITI) has begun modernizing the country's digital certification infrastructure to adapt to advances in quantum computing. A Normative Instruction published this week establishes the adoption of post-quantum cryptographic algorithms in the Brazilian Public Key Infrastructure (ICP-Brasil).

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 6, 2026

EL SALVADOR FACES GLOBAL CYBERATTACKS: WHY CYBERSECURITY IS THE NEW PILLAR OF NATIONAL DEVELOPMENT

Infobae - Most incidents originate outside the country, bypassing national legal controls; experts warn that strengthening regulations and raising awareness about digital footprints are key to the economic and social future. The growth of cybercrime and the sophistication of digital attacks are now a major concern in Salvadoran society. Experts noted that online fraud has not only increased in number, but also in complexity and scope, affecting both businesses and individuals.

CYBERSECURITY AND TRACEABILITY: THE CHALLENGE THAT IS REDEFINING LOGISTICS SECURITY IN CHILE

Innova Portal - In a context of growing digital threats and increased regulatory demands, supply chain security has become critical for Chilean foreign trade. ISO 28000 certification is consolidating itself as a key standard for strengthening traceability, operational continuity, and cybersecurity in the off-dock sector. February 2026. The increase in digital threats, operational disruptions linked to criminal organizations, and stricter regulations have elevated logistics security to a strategic level in Chile. For companies operating critical infrastructure, the challenge is no longer limited to protecting cargo, but also to guaranteeing traceability, continuity, and cybersecurity throughout the entire operational flow.

ECUADOR PRESENTS ITS PUBLIC POLICY FOR THE ETHICAL DEVELOPMENT OF AI

dpl News - Ecuador officially presented the Strategy for Promoting the Development and Ethical and Responsible Use of Artificial Intelligence, an instrument the government had been working on since August of last year. This strategy aims to establish a public policy to organize, guide, and accelerate the adoption of this technology in the country, prioritizing the protection of fundamental rights, social inclusion, and environmental sustainability. Issued by the Ministry of Telecommunications and the Information Society (MinTEL) and published in the Official Gazette in January 2026, the strategy incorporates a four-year implementation vision (2025–2029) and focuses on the development and use of Artificial Intelligence (AI) to contribute to social well-being.

CYBERSECURITY 2026: TRENDS AND WHY IT MATTERS TO BUSINESS

El Heraldo - 2026 marks a turning point for cybersecurity. This year is about adding technology while simultaneously transforming how organizations understand, manage, and address risk. Innovation, the widespread use of artificial intelligence, and the interconnectedness of digital ecosystems are redefining how value is created and protected. The World Economic Forum's (WEF) Global Cybersecurity Outlook 2026 describes a scenario driven by three pillars: the constant increase in threats, geopolitical fragmentation that hinders international cooperation, and a persistent technology gap between organizations. Amidst this, artificial intelligence acts as a cross-cutting enabler. It increases productivity and defensive automation, but it also opens up new attack vectors and risks that are difficult to anticipate.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 6, 2026

LATAM-GPT: THE FIRST ARTIFICIAL INTELLIGENCE WITH A LATIN AMERICAN IDENTITY

24 Hours - The official launch of Latam-GPT, the first open Grand Language Model (LLM) designed entirely from and for Latin America and the Caribbean, will take place next Tuesday, February 10. This technological milestone represents the most ambitious collaborative Artificial Intelligence project in the region, positioning the continent's countries not only as users but also as active developers of cutting-edge technology. Latam-GPT was created as a public good aimed at democratizing access to the enabling infrastructure necessary for regional competitiveness, and its importance lies in the urgent need to achieve technological and cultural sovereignty in a context where Artificial Intelligence is redefining the margins of global productivity.

CISA ORDERS FEDERAL AGENCIES TO STRENGTHEN EDGE DEVICE SECURITY AMID RISING CYBER THREATS - USA

CISA.gov - The Cybersecurity and Infrastructure Security Agency (CISA) today issued Binding Operational Directive 26-02, Mitigating Risk From End-of-Support Edge Devices. The directive requires Federal Civilian Executive Branch (FCEB) agencies to take specific actions to drive down technical debt and minimize the risk of compromise. Within a specified timeframe, FCEB agencies must strengthen asset lifecycle management for active edge devices and remove any hardware and software devices that is no longer supported by its original equipment manufacturer. Persistent cyber threat actors are increasingly exploiting unsupported edge devices - hardware and software that no longer receive vendor updates to firmware or other security patches. Positioned at the network perimeter, these devices are especially vulnerable to persistent cyber threat actors exploiting a new or known vulnerability. To mitigate this threat, CISA is requiring FCEB agencies to adhere to standard lifecycle management processes and mandatory actions within the required time limit in this directive.

FCC ISSUES CYBERSECURITY BEST PRACTICES FOR DEFENDING AGAINST RANSOMWARE ATTACKS - USA

DWT - The Federal Communications Commission's (FCC) Public Safety and Homeland Security Bureau (Bureau) recently released a public notice (Notice) emphasizing the threat of ransomware to communications networks and urging providers to adopt various cybersecurity best practices. The Notice, dated January 29, 2026, is geared toward small-to-medium sized providers, but its recommendations are relevant to larger providers as well. The Bureau's guidance underscores that providers of all sizes, including those with potentially more limited technical and financial resources, have been targeted by ransomware actors and have faced significant operational disruption, data loss, and public safety impacts as a result.

NATIONAL CYBERSECURITY STRATEGIES DEPEND ON PUBLIC-PRIVATE TRUST, REPORT WARNS

Cybersecurity Dive - Governments should work closely with the private sector when designing and detailing their national cybersecurity strategies, a prominent think tank said in a report published on Monday. “Active participation from the private sector, particularly large technology, telecommunications, and cybersecurity firms, is critical throughout the strategy’s development,” the Center for Cybersecurity Policy and Law (CCPL) said in its white paper. “The private sector can help not only support but also deliver on the government’s cybersecurity objectives and is key to a secure and resilient nation.”