DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 12, 2026

DIGI AMERICAS ALLIANCE MEMBERS

ASSEMBLY APPROVES BILL FOR THE STRENGTHENING OF CYBERSECURITY - ECUADOR

AsambleaNacional.gob.ec - The Plenary of the Assembly, this Tuesday, February 10, with 82 affirmative votes, approved the Organic Law project for the Strengthening of Cybersecurity, which creates a modern, technically founded and constitutionally compatible architecture to strengthen national cybersecurity, articulate a coherent model of digital governance, protect critical infrastructure and guarantee continuity of essential services.

THE GOVERNMENT LAUNCHED THE NATIONAL CYBERSECURITY CENTER AND APPOINTED ITS AUTHORITIES - ARGENTINA

Filo.news - The government has officially created the National Cybersecurity Center (CNC), a new state agency tasked with safeguarding the State's digital assets and systems linked to essential public services. The measure was established through Decree 941/2025 and is part of the amendment to the Intelligence Law. The CNC will report to the Secretariat of Innovation, Science and Technology within the Chief of Staff's Office and will be responsible for protecting critical information infrastructure, as well as preventing and responding to cybercrimes that could compromise sensitive files or strategic networks. Ariel Waissbein has been appointed to head the agency.

WE LAUNCHED LATAM-GPT: THE FIRST ARTIFICIAL INTELLIGENCE CREATED FOR LATIN AMERICA AND THE CARIBBEAN - CHILE

Gob.cl - Chile is once again at the forefront of regional technology thanks to the launch of Latam-GPT, the first major open language model designed specifically for Latin America and the Caribbean, a ceremony led by President Boric. Latam-GPT aims to build Chile's own capabilities in generative artificial intelligence, promoting ethical governance and an open architecture that respects our culture and local contexts.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 12, 2026

COLOMBIA: NEW ALLIANCE WITH CHILE WILL BOOST ARTIFICIAL INTELLIGENCE AND SUPERCOMPUTING IN LATIN AMERICA

trendTIC - Colombia and Chile consolidate a strategic alliance in Science, Technology, and Innovation, with an emphasis on artificial intelligence and supercomputing, through the signing of a Memorandum of Understanding between the Colombian Ministry of Information and Communications Technologies (ICT) and the Chilean Ministry of Science, Technology, Knowledge, and Innovation. This collaboration aims to advance technological sovereignty and strengthen digital capabilities in the region. With this agreement,

MEXICAN PUBLIC SECTOR FACES LEAKS, RANSOMWARE AND COMPROMISED CREDENTIALS

The Economist - January 2026 revealed that the public sector in Mexico is exposed to a recurring pattern: the risk is no longer explained solely by hacking, understood as sophisticated technical exploitation, but by a combination of legacy systems, outsourced operations, weak identity management, and a password culture that makes account theft likely. In this combination, the damage doesn't always occur in the core infrastructure, but rather at the edges of the digital state, in old applications that remain active, access points that remain enabled, and exposed repositories that can be downloaded en masse.

CYBER DEFENSE COMMAND PRESENTS STRATEGIC PERFORMANCE DURING INSTITUTIONAL VISIT

Brazilian Army - The Cyber Defense Command (ComDCiber) is the central body of the Military Cyber Defense System (SMDC) and is part of the Brazilian Army's structure, being responsible for planning, coordinating, and conducting Cyber Defense actions. Its work focuses on protecting critical infrastructure, information systems, and strategic assets of the country. During the meeting, members of the Judiciary had the opportunity to learn about the relevance of Cyber Defense to national security, especially regarding the protection of systems, strategic information, and ensuring the safe, reliable, and effective use of cyberspace.

LATIN AMERICA ON ALERT: ALMOST 38% OF GLOBAL CYBER THREATS OPERATE UNDETECTED

Forbes Central America – “The biggest risk today isn’t the attack that triggers alerts, but the one that manages to go undetected,” warned Ricardo Villadiego, founder and CEO of Lumu Technologies, emphasizing that a growing number of current intrusions manage to evade preventative controls and remain active for extended periods without being identified. The report specifies that 18.9% of detections correspond to active malicious behavior, while 18.7% are linked to operational phishing domains. These two categories reflect activities that go beyond attempts blocked at the perimeter, directly impacting organizations’ internal environments.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 12, 2026

CHINESE CYBERSPIES BREACH SINGAPORE'S FOUR LARGEST TELCOS

Bleeping Computer - The Chinese threat actor tracked as UNC3886 breached Singapore's four largest telecommunication service providers, Singtel, StarHub, M1, and Simba, at least once last year. The hackers also gained limited access to critical systems but did not pivot deep enough to disrupt services. In response to the intrusions, which were disclosed in July 2025, Singapore deployed 'Operation Cyber Guardian' to limit the adversary's activity on the telco's networks, but very few details were shared at the time. "Over the past months, our investigations have indicated that UNC3886 had launched a deliberate, targeted, and well-planned campaign against Singapore's telecommunications sector," Singapore's Cyber Security Agency (CSA) states.

GLOBAL CYBERSECURITY OUTLOOK 2026 REGIONAL ANALYSES

World Economic Forum - Cybersecurity risk in 2026 is accelerating, driven by rapid advances in artificial intelligence, deepening geopolitical fragmentation and increasingly complex supply chains. These regional analyses build on the Global Cybersecurity Outlook 2026 to explore how these global dynamics are unfolding across different parts of the world, offering a focused view of each region's evolving cybersecurity landscape.

CLOSING THE CYBER EQUITY GAP: HOW COLLECTIVE INVESTMENT CAN SECURE THE INTERNET FOR EVERYONE

World Economic Forum - Cybercrime is often seen as a tug-of-war: criminals innovating to stay ahead of countermeasures, while governments work to hold criminals accountable. The private sector tends to sit in the middle, trying to maximize profit while protecting customers and complying with law enforcement. Nonprofit organizations, however, also have a quiet but essential role in keeping the internet secure. For example, standards bodies develop the technical protocols that allow networks to interoperate safely. Open-source projects maintain critical cybersecurity tools. Infrastructure nonprofits safeguard the naming, numbering and routing systems that underpin the internet's functionality.

HACKTIVISTS, STATE ACTORS, CYBERCRIMINALS TARGET GLOBAL DEFENSE INDUSTRY, GOOGLE WARNS

Security Week - Google warns of escalating, multifaceted cyber threats targeting the global DIB, including contractors, suppliers, and personnel supporting military capabilities. The analysis highlights a "relentless barrage" of cyber operations from state-sponsored actors linked to China, Russia, Iran, and North Korea; pro-Russia and pro-Iran hacktivists; and cybercriminals, particularly groups launching ransomware attacks on manufacturing. China-nexus cyberespionage dominates in volume, often exploiting edge devices and zero-days for long-dwell intrusions into aerospace and defense entities. Groups conducting such operations include UNC4841, UNC3886 (blamed for the recent Singapore telecom attacks), and UNC5221.

HOW RANSOMWARE HACKERS CHOOSE THEIR VICTIMS

Cybersecurity Insiders - Ransomware attacks have become one of the most profitable forms of cyber-crime. Instead of randomly infecting computers, modern ransomware groups operate like businesses. They carefully select their targets to maximize profit while minimizing risk. Understanding how these hackers choose victims reveals why certain organizations are repeatedly attacked.