DIGI AMERICAS ALLIANCE MEMBERS

Apple aws Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE
fluid attacks we hack your software Google kriptos LUMU netskope paloalto NETWORKS
Resecurity Schneider Electric SISAP Sistemas Aplicativos SOPHOS tenable Trellix TrendAI

MEXICO ESTABLISHES FIRST NATIONAL COMMITTEE FOR COMPETENCY-BASED MANAGEMENT IN CYBERSECURITY

eSemanal - Experts from the public, private, and academic sectors have established the first Cybersecurity Competency Management Committee under the National Competency System (CONOCER). The committee aims to develop official standards to professionalize talent through certifications that serve as a skills passport, strengthening job mobility within the distribution channel.

PARAGUAY AND POLAND STRENGTHEN COOPERATION IN SECURITY AND CYBERSECURITY

Mas Encarnación - During the meeting, opportunities for cooperation between Paraguay and Poland were discussed in key areas such as security, cybersecurity, and hybrid threats, with the aim of strengthening the exchange of experiences and institutional collaboration between the two countries. Interior Minister Enrique Riera Escudero led a meeting with Polish Deputy Foreign Minister Wojciech Zajączkowski and his delegation at the Ministry headquarters, accompanied by Deputy Minister of Political Affairs Oscar Campuzano. During the meeting, opportunities for bilateral cooperation in strategic areas such as security, cybersecurity, and hybrid threats were analyzed.

COLOMBIA: PETRO GOVERNMENT PRESENTS ROADMAP TO MODERNIZE SPECTRUM MANAGEMENT IN COLOMBIA BETWEEN 2026 AND 2029

trendTIC - At a crucial moment for connectivity and digital adaptation in the country, Colombia has consolidated a new proposal for managing one of the most strategic resources in its technological ecosystem: the Spectrum Management Policy 2026-2029, led by the Ministry of Information and Communications Technologies (ICT) and the National Spectrum Agency (ANE). The document, which proposes a more efficient and innovative management environment capable of responding to industry transformations, the needs of the State, and the urgent need to close digital divides with modern and sustainable tools, was presented by ICT Minister Carina Murcia at Andina Link 2026, held in Cartagena.

DIGI AMERICAS LATAM CISO

INSIGHTS

MARCH 12, 2026

CHILE-CHINA SUBMARINE CABLE OPENS DEBATE ON DIGITAL SOVEREIGNTY AND DATA SECURITY

Portal Innova - The submarine cable project seeking to directly connect Chile with Asia, and particularly with China, has reignited a strategic debate about the security of the data that will travel through this critical infrastructure. Although the public discussion is focused on the fiber optic cable installed on the ocean floor, cybersecurity specialists warn that the real vulnerability lies in the software systems that manage and control communications traffic. The initiative is part of efforts to strengthen Chile's digital connectivity and consolidate its position as a technological hub in Latin America, reducing dependence on routes that currently pass primarily through the United States. However, specialists argue that the discussion should not be limited to the physical infrastructure, but should also consider who controls the technological platforms that operate the network.

AI REGULATION IN BRAZIL ENTERS POLITICAL DEBATE IN THE CHAMBER OF DEPUTIES

Economic News Brazil - AI regulation in Brazil returned to the center of the legislative agenda this Monday (March 9th), after the topic was included among the priorities of the Chamber of Deputies. The bill that establishes rules for the use of artificial intelligence still faces disagreements within the federal government and pressure from technology companies, while the rapporteur, Deputy Aguinaldo Ribeiro (PP-PB), prepares the presentation of his report. The text arrived at the Chamber in early 2025 and remains without public disclosure. Even so, Ribeiro stated that he intends to bring the proposal to a vote in the special committee in April. The debate involves defining limits for artificial intelligence systems, protecting fundamental rights, and stimulating technological development in the country.

CIOS PRIORITIZE CYBERSECURITY AND DATA MANAGEMENT IN INVESTMENTS FOR 2026 - BRAZIL

itforum - While companies are expanding their adoption of artificial intelligence (AI) to increase efficiency and productivity, they are also expanding its attack surface, creating opportunities for attackers. Without a resilient infrastructure and digital governance, AI ceases to be an engine of innovation and becomes a strategic target for cyberattacks and manipulation. Brazilian CIOs are aware of this challenge. Effective data management, which involves collection, storage, classification, and secure disposal, provides the necessary foundation for cybersecurity to implement more precise protections, preventing leaks and ensuring compliance with regulations such as the LGPD (Brazilian General Data Protection Law).

BETWEEN COMPREHENSIVE PROTECTION, RESPONSIVE GOVERNANCE, AND DIGITAL EDUCATION - BRAZIL

Diplomatique Brasil - Amidst a contemporary debate on the challenges of protecting children and adolescents in the digital environment, the enactment of the so-called Digital ECA (Law No. 15.211/2025), scheduled to come into force on March 18, gains relevance. This article proposes an analysis of this legislation from three perspectives: comprehensive protection, responsive regulatory governance, and digital education. More than describing the law, it is important to understand what its creation and implementation reveal about the state of Brazilian regulation in an environment marked by informational asymmetries, data-driven business models, and algorithmic systems geared towards capturing attention.

DIGI AMERICAS LATAM CISO

INSIGHTS

MARCH 12, 2026

REPORT SAYS RISE IN AI FAILURES ALERTS GLOBAL CYBERSECURITY

Nanche Michoacan – The number of AI-related vulnerabilities could exceed 3,000 by 2026, making it one of the main cybersecurity risks. Mexico City. The accelerated adoption of artificial intelligence (AI) is generating critical challenges in global cybersecurity, according to the report 'Fault Lines in the AI Ecosystem' by TrendAI, with an increase of almost 35% in 2025 compared to the previous year. This document revealed that 2,130 AI-related vulnerabilities were registered in 2025, a 34.6% increase compared to the previous year, representing 4.42% of all software vulnerabilities detected globally. The analysis warned that, if the trend continues, the number of AI-related vulnerabilities could range between 2,800 and 3,600 by 2026, solidifying it as one of the main risks in the global cybersecurity landscape.

WHITE HOUSE UNVEILS CYBER STRATEGY TO STRENGTHEN WORKFORCE AND NATIONAL SECURITY - USA

The Cyber Edge - The new Cyber Strategy for America, released on March 6 by the White House, outlines an approach to cybersecurity that emphasizes a proactive and unified stance across federal, state, local, tribal and private sector partners. The strategy also signals an emphasis on workforce development, including plans for a cyber academy to train the next generation of cybersecurity professionals. White House National Cyber Director Sean Cairncross described the strategy as a road map to better align federal resources and interagency actions and deepen collaboration with industry, state and local partners to counter evolving cyber threats.

WHITE HOUSE ISSUES EXECUTIVE ORDER ADDRESSING CYBERCRIME BY THREAT GROUPS - USA

American Hospital Association - The White House issued an executive order March 6 to combat cybercrimes by threat groups. The order highlights how such groups can receive willing or tacit state support for cyberattacks involving ransomware and malware, phishing, financial fraud and other schemes. The order directs federal agencies within 120 days to create an action plan that would be carried out by the National Coordination Center to identify criminal organizations “responsible for scam centers and cybercrime” and to propose solutions to dismantle those groups. The plan would describe how the attorney general and the secretary of Homeland Security should use technological capabilities, threat intelligence and operational insights from cybersecurity firms and other non-federal entities to improve attribution, tracking and disruption of cybercriminal activity. The plan would also include mechanisms to improve information sharing, operational coordination and rapid response across the federal government.

CYBERSECURITY IN CONNECTED MEDICAL DEVICES: A POLICY AGENDA FOR THE NHS - USA

Nature - Connected Medical Devices (CMD) are redefining care within the NHS but exposing it to bi-directional cyber-physical threats that traverse physical, network and cloud layers. These vulnerabilities blur the boundary between technology and patient safety. This Comment argues that the MHRA should elevate cybersecurity to a clinical-safety mandate, enforcing a unified socio-technical framework with security-by-design, cross-layer risk assessment and continuous post-market vigilance.