DIGI AMERICAS ALLIANCE MEMBERS

CHILE | SENATORS PROPOSE REGULATING THE ETHICAL USE OF AI IN BIOMEDICAL RESEARCH

DPL News - Bill seeks to balance scientific advancement and the protection of individual rights in Chile. It establishes guiding principles such as transparency and non-discrimination. It requires authorization from ethics committees for AI research. It mandates constant human oversight of AI systems. It obliges institutions to assess and mitigate risks, especially algorithmic bias. It strengthens the protection of personal data and informed consent. It introduces penalties for non-compliance.

CYBERSECURITY AS A MATTER OF NATIONAL SECURITY - MEXICO

El Heraldo - The publication of the National Cybersecurity Plan 2025–2030 represents a turning point for Mexico's national security. For the first time, the State explicitly recognizes that cyberspace has become a strategic domain where criminal, economic, political, and geopolitical risks converge. In an international environment marked by technological competition, digital fragmentation, and the use of cyberspace as an instrument of power, this recognition is late, but essential.

MEXICO AND ESTONIA WILL SEEK EXCHANGES ON GOVERNMENT DIGITIZATION AND CYBERSECURITY

Diario Noticias - Upon the installation of the Mexico-Republic of Estonia Friendship Group, its president, Deputy Deliamaria González Flandez (PVEM), mentioned that its purpose will be the exchange in matters of government digitization, cybersecurity, technological training and electronic commerce. The legislator indicated that the relationship between the two nations is based on shared values and a common vision for the future.

DIGI AMERICAS LATAM CISO

INSIGHTS

DECEMBER 26, 2025

BETWEEN CHIPS, DATA, AND ARTIFICIAL INTELLIGENCE, 2025 MARKED THE ADVANCEMENT OF BRAZIL'S TECHNOLOGICAL SOVEREIGNTY

Gov.br - When it comes to technological sovereignty, 2025 was a year in which Brazil decided to accelerate its pace — and it did so with method, investment, and a vision for the future. Under the coordination of the Ministry of Science, Technology and Innovation (MCTI), the country ended the year with R$ 267 million invested in strategic ICT projects, a 116% increase in funding compared to 2024, in addition to an institutional framework that began operating at a pace compatible with the challenges of the digital age. In a world where data, chips, artificial intelligence, and supercomputing define power and autonomy, the ministry transformed public policy into concrete infrastructure for national development.

CYBERSECURITY BUDGETS IN 2026: PERSPECTIVES FOR BRAZIL

Computer Weekly - In many sectors of the economy, cybersecurity budgets in 2025 were conservative, more focused on maintaining existing defenses than on genuine innovation. A report by IANS Research with US CFOs from various verticals revealed that, on average, cybersecurity budgets increased by only 4% compared to 2024. This represents 50% of the average 8% growth in these investments over the last five years. The focus was on maximizing the resources that companies already possessed. In Brazil and Latin America, in particular, the situation is even more complex. There is underinvestment in cybersecurity that weakens governments and companies, making the region a prime target for criminals.

CYBERSECURITY MATURITY IS IMPROVING IN LATIN AMERICA AND THE CARIBBEAN, ACCORDING TO A REPORT BY THE IDB AND THE OAS

DPL News – Latin American and Caribbean countries have made significant progress in strengthening their cybersecurity capabilities, but disparities in resources, talent development, and intersectoral coordination persist, leaving the region vulnerable to evolving digital threats, according to a new report by the Inter-American Development Bank (IDB) and the Organization of American States (OAS). The report, “Cybersecurity 2025: Vulnerability and Maturity Challenges to Reduce Gaps in Latin America and the Caribbean,” produced in collaboration with the Global Cyber Security Capacity Centre at the University of Oxford, offers the most comprehensive assessment to date of cybersecurity maturity in 30 countries across the region. The study compares national capabilities using the Cybersecurity Capacity Maturity Model for Nations (CMM), enabling comparative analysis over time and across countries.

LATIN AMERICA FACES GENAI AND FINTECH RISKS IN 2026

Mexico Business - For 2026, the stability of Latin America’s financial sector will hinge on managing risks arising from generative AI (GenAI), disparities in regional regulatory maturity, and the growing interconnectivity of Fintech ecosystems. Systemic vulnerability is not confined to isolated attack vectors but emerges from sophisticated, cross-cutting threats. This view highlights a shift from a reactive defensive posture to an operational resilience model focused on response capacity and adaptability to complex incidents. The 2026 risk landscape is shaped by technologies that have transformed the traditional security perimeter. The acceleration of GenAI has democratized tools that once required advanced expertise, fueling hyper-personalized phishing campaigns and high-fidelity deepfakes targeting biometric authentication and social engineering protocols

COLLINS' CYBERSECURITY INITIATIVE FOR ELECTIONS ENACTED IN MAJOR DEFENSE LEGISLATION - USA

RSWEBSOLS - Legislation, spanning party lines, spearheaded by U.S. Senators Susan Collins (R) and Mark Warner (D) to enhance the security of American elections, has received presidential approval as an integral component of the Fiscal Year 2026 National Defense Authorization Act (NDAA). The election security initiative is rooted in the Strengthening Election Cybersecurity to Uphold Respect for Elections through Independent Testing (SECURE IT) Act, introduced by Collins and Warner in May. This legislation's provisions were seamlessly woven into the annual defense authorization, mandating the Election Assistance Commission to implement penetration testing for election systems aiming for federal certification.

HARMONIZING COMPLIANCE: HOW OVERSIGHT MODERNIZATION CAN STRENGTHEN AMERICA'S CYBER RESILIENCE

Federal News Network - For decades, the federal government has relied on sector-specific regulations to safeguard critical infrastructure. As an example, organizations including the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) set standards for the energy sector, while the Transportation Security Administration issues pipeline directives and the Environmental Protection Agency makes water utility rules. While these frameworks were designed to protect individual sectors, the digital transformation of operational technology and information technology has made such compartmentalization increasingly risky.

AGENCIES ACROSS AFRICA ARREST 574, RECOVER $3 MILLION IN CYBERCRIME CRACKDOWN

The Cyber Express - Law enforcement across 19 African countries arrested 574 suspects and recovered approximately $3 million in a month-long cybercrime crackdown, dubbed Operation Sentinel. The operation primarily targeted three forms of cybercrimes – business email compromise schemes, digital extortion, and ransomware attacks. Interpol, who coordinated the logistics of this operation revealed that these operations costed Africans financial losses that exceeded $21 million.

QUANTUM-RESISTANT CYBERSECURITY ADVANCES PROTECTION AGAINST SHOR AND GROVER ALGORITHM THREATS

Quantum Zeitgeist - The increasing power of computers poses a significant threat to current cybersecurity protocols, as they become vulnerable to sophisticated algorithms capable of breaking existing encryption. Navin Chhibber from Infinity Tech Group, Amber Rastogi, Ankur Mahida from Barclays, and Vatsal Gupta et al. address this challenge by investigating quantum-resistant cryptographic models, also known as post-quantum cryptography. Their work explores the design, implementation, and testing of robust algorithms based on approaches such as lattice, code, polynomial, and hash-based cryptography, evaluating their resilience against both conventional and quantum attacks. This research demonstrates the potential to build amplified security for future cybersecurity systems, including applications in secure communications, blockchain technology, and cloud computing, while also proposing a hybrid model that combines existing and quantum-resistant methods for a seamless transition and enhanced forward security.