DIGI AMERICAS ALLIANCE MEMBERS

MEXICO PRESENTS ITS FIRST NATIONAL CYBERSECURITY PLAN AND IS PURSUING A GENERAL LAW

Wired - Mexico is looking to move from a reactive to a proactive approach in the digital realm. The Agency for Digital Transformation and Telecommunications (ATDT) presented the National Cybersecurity Plan this Thursday, the first state policy specifically designed to standardize the defense of critical infrastructure and government systems. The goal is to reduce the attack surface and finally establish true "cyber resilience" in the region. This is not just about good intentions; the plan includes the creation of a General Cybersecurity Law and mandatory measures that will be published this year.

DATA CENTERS IN MEXICO: MODERNITY, RISKS AND THE STRATEGIC ROLE OF ELECTRONIC SECURITY

Segurilatam - The rapid growth of data centers in Mexico is redefining the physical and technological security needs of the industry. Between 2025 and 2030, investment in data center infrastructure is estimated to reach $18 billion, representing unprecedented expansion and an additional capacity of over 1,500 MW in operation. This evolution, driven by the cloud, massive storage, and the growing demand for artificial intelligence, is transforming data centers into true critical infrastructure for the country.

BRAZILIAN GOVERNMENT SENDS DRAFT BILL TO CONGRESS TO CREATE THE NATIONAL ARTIFICIAL INTELLIGENCE SYSTEM

Capital Digital - The President of the Republic, Luiz Inácio Lula da Silva, sent to the National Congress, this Monday evening (08), in an extra edition, Message number 1845 of December 8, 2025 with the text of the Bill that establishes the “National System for the Development, Regulation and Governance of Artificial Intelligence”. The sending marks another move by the federal government to structure a comprehensive public policy aimed at organizing the expansion of the AI ecosystem in the country amidst the accelerated advancement of this technology in the productive sectors, in public administration and in essential services.

SENATE ADVANCES NATIONAL POLICY FOR DIGITAL PROTECTION OF PUBLIC SERVICES - BRAZIL

Senate - The creation of a national policy to protect public data and keep essential services running in the event of digital attacks took another step forward in the Senate. The Constitution and Justice Committee (CCJ) approved this Wednesday (10) the bill that establishes the legal framework for cybersecurity and the National Program for Digital Security and Resilience. PL 4.752/2025, by Senator Esperidião Amin (PP-SC), received a favorable opinion from Senator Hamilton Mourão (Republicanos-RS) and will proceed to final analysis by the Science and Technology Committee (CCT).

BOLIVIA AND SPAIN CONSOLIDATE BILATERAL COOPERATION AGENDA ON SECURITY

eju.tv - Spain has pledged to provide technical assistance, promote the establishment of data centers, and share police technology developed in conjunction with other Ibero-American forces. The agreement was formalized by the Secretary General of the Vice Presidency of Bolivia, Iván Montoya, and the Director General of the Spanish National Police, Francisco Pardo, during a meeting at the Spanish police headquarters. During the meeting, the officials agreed that organized crime and transnational crime require joint responses, emphasizing the continued relevance of the existing cooperation agreement between the two countries.

SIX TRENDS THAT WILL SHAPE CYBERSECURITY IN THE AGE OF AI IN 2026

Forbes predicts that 2026 will be the "Year of the Defender," where autonomous AI defense will be the only way to combat AI-driven identity attacks, data poisoning, and quantum risks. Palo Alto Networks (NASDAQ: PANW) published "6 Predictions for the AI Economy: The New Rules of Cybersecurity in 2026," forecasting a transformative leap toward an AI-driven economy. This new, AI-native global economic model, where AI drives productivity and operations, also introduces a seismic shift in risk.

AGENTIC AI IS THE NEW FRONTIER FOR BOOSTING PRODUCTIVITY IN LATIN AMERICA: AWS

DPL News – Amazon Web Services (AWS) has described Aggressive Artificial Intelligence as the “new frontier” and a new opportunity for the region to address local challenges through innovation. To capitalize on this opportunity, the company has accelerated its investments in the region, including $5 billion for the deployment of a region in Mexico and the upcoming launch of a new region in Chile in 2026. AWS projects that Aggressive AI will be integrated into 33% of enterprise applications by 2028 and will influence 15% of daily business decisions.

OPPORTUNISTIC PRO-RUSSIA HACKTIVISTS ATTACK US AND GLOBAL CRITICAL INFRASTRUCTURE

CISA - CISA, in partnership with Federal Bureau of Investigation, the National Security Agency, Department of Energy, Environmental Protection Agency, the Department of Defense Cyber Crime Center, and other international partners published a joint cybersecurity advisory, Pro-Russia Hacktivists Create Opportunistic Attacks Against US and Global Critical Infrastructure. This advisory, published as an addition to the joint fact sheet on Primary Mitigations to Reduce Cyber Threats to Operational Technology (OT) released in May 2025, details that pro-Russia hacktivist groups are conducting less sophisticated, lower-impact attacks against critical infrastructure entities, compared to advanced persistent threat groups.

KEY CYBERSECURITY TAKEAWAYS FROM THE 2026 NDAA - USA

CSO - On Dec. 7, the House and Senate Homeland Security Committees released their compromise version of the 2026 National Defense and Authorization Act (NDAA), a nearly 3,100-page piece of legislation that contains a host of provisions to fund several Department of Defense cybersecurity efforts in fiscal year 2026. Although cybersecurity is referenced hundreds of times across the NDAA, the legislation contains provisions that, once the law becomes effective, will mark significant shifts in how the US military manages major cybersecurity tasks, particularly in the timely arena of protecting mobile communications of top brass and AI deployments, as well as more understated, but potentially high-impact, infosec duties.

CYBER THREATS TO THE U.S.: WHAT POLICYMAKERS NEED TO KNOW FOR 2026

Check Point - Cyber attacks against the United States are no longer isolated events or technical headaches. They are now powerful tools of national strategy used by foreign governments, criminal networks, and ideological groups. A new report explains how these attacks have changed from simple hacks into coordinated campaigns aimed at shaping global politics, weakening U.S. institutions, and putting pressure on American decision-makers.
This blog highlights the key takeaways for leaders responsible for national security, public policy, and critical infrastructure resilience.

NUCLEAR CYBERSECURITY RESEARCHERS AND INDUSTRY UNITE TO PROTECT NEXT-GEN REACTORS

INL - As the United States accelerates deployment of advanced and small modular reactors (A/SMRs), the nuclear energy sector is embracing a digital future. While digital systems provide operators with big benefits, they can also create vulnerabilities that enable criminals to access critical infrastructure. To protect the next generation of reactors, cybersecurity has become a critical pillar of trust, safety and resilient operations. “Cybersecurity can’t be an afterthought — it needs to be discussed and implemented now,” said J’Tia Hart, the Nuclear Nonproliferation division director at the Idaho National Laboratory (INL).

APPLE, GOOGLE SEND NEW ROUND OF CYBER THREAT NOTIFICATIONS TO USERS AROUND WORLD

Reuters - Apple (AAPL.O), opens new tab and Google have sent a new round of cyber threat notifications to users around the world, the companies said this week, announcing their latest effort to insulate customers against surveillance threats. Apple and the Alphabet-owned (GOOGL.O), opens new tab Google are two of several tech companies that regularly issue warnings to users when they determine they may have been targeted by state-backed hackers. Apple said the warnings were issued on Dec. 2 but gave few further details about the alleged hacking activity and did not address questions about the number of users targeted or say who was thought to be conducting the surveillance. Apple said that "to date we have notified users in over 150 countries in total." Apple's statement follows Google's Dec. 3 announcement, opens new tab that it was warning all known users targeted using Intellexa spyware, which it said spanned "several hundred accounts across various countries, including Pakistan, Kazakhstan, Angola, Egypt, Uzbekistan, Saudi Arabia, and Tajikistan."