DIGI AMERICAS LATAM CISO

INSIGHTS

DECEMBER 18, 2025

DIGI AMERICAS ALLIANCE MEMBERS

ATDT ISSUES GENERAL CYBERSECURITY POLICY FOR THE FEDERAL PUBLIC ADMINISTRATION - MEXICO

La Jornada - The Digital Transformation and Telecommunications Agency today issued the Agreement establishing the General Cybersecurity Policy for the Federal Public Administration. In the document published in the Official Gazette of the Federation, the agency, headed by José Antonio Peña Merino, stated that the magnitude of digital threats is undeniable and that, according to the Fortinet Global Threat Landscape Report 2025, Mexico registered more than 324 billion attempted cyberattacks during 2024, placing the country among the most threatened in Latin America.

MEXICO IS ACCELERATING THE ADOPTION OF ARTIFICIAL INTELLIGENCE, CYBERSECURITY, QUANTUM TECHNOLOGIES, AND HYBRID CLOUD

Comunicae – Mexico is consolidating its leadership in technological innovation in Latin America, with increasing adoption of artificial intelligence (AI), advanced cybersecurity, quantum computing, intelligent automation, and 5G connectivity. The report highlights that more than 60% of Mexican companies are accelerating their digital transformation, driven by the need to increase productivity, strengthen operational resilience, and respond to a highly competitive global environment. Initiatives such as the National Digital Agenda, the 2024-2030 Cybersecurity Strategy, and industrial innovation programs have been key factors in this progress.

CHILE PUBLISHES THE FIRST GROUP OF INSTITUTIONS CLASSIFIED AS VITAL OPERATORS

Segurilatam - The Official Gazette of the Republic of Chile published, on December 17, the list of critical operators in the electricity, telecommunications, digital services, banking and financial institutions, healthcare providers, public companies, and government agencies sectors. Of the 1,712 institutions preliminarily assessed, 915 were declared by the National Cybersecurity Agency (ANCI) as critical operators for the country's cybersecurity.

DIGI AMERICAS LATAM CISO

INSIGHTS

DECEMBER 18, 2025

SENATE APPROVES LEGAL FRAMEWORK FOR DIGITAL PROTECTION AND STRENGTHENS CYBERSECURITY AGENDA FOR THE BRAZILIAN MARKET

Segs - New policy marks institutional progress amid escalating digital attacks, but experts warn of the challenge of transforming guidelines into effective protection. In a scenario where Brazil faces thousands of cyberattack attempts each year, the Federal Senate took a strategic step by approving, this past Wednesday (10), the creation of the National Digital Protection Policy. The measure, which now goes to the Science and Technology Committee (CCT) for analysis, seeks to increase the country's resilience in the face of a continuously growing volume of threats, with direct impacts on essential public services and critical infrastructure chains.

BRAZILIAN ARMY PROMOTES INTEGRATION FOR THE DEVELOPMENT OF STRATEGIC CYBERSECURITY SOLUTIONS - BRAZIL

Defesanet - The Army General Staff (EME), in partnership with the Higher School of Defense (ESD), held a Cybersecurity Workshop with the objective of identifying opportunities, synergies, and models for joint action aimed at developing strategic solutions for the digital environment. The meeting brought together representatives from public, private, and academic institutions, expanding the dialogue on challenges and needs in the area. During the workshop, specialists presented analyses and experiences related to the evolution of digital threats, risk management, and trends in technological innovation.

BRAZIL LAUNCHES ITS FIRST ARTIFICIAL INTELLIGENCE MODEL TRAINED 100% IN PORTUGUESE

DPL News - Brazil presented its first Artificial Intelligence model developed and trained entirely in Portuguese on Tuesday, December 9. Named SoberanIA, the project was launched during the National Meeting on Sovereign AI in Brasília and brings together the Ministry of Science, Technology and Innovation, the government of the state of Piauí, Telebras, the Federal University of Piauí, and the companies Modular and Scala Data Centers. As the project's name suggests, the initiative addresses the practical issue of digital sovereignty.

FROM AI THREATS TO QUANTUM SECURITY: CYBERSECURITY TRENDS IN 2026

Forbes Brazil - As the digital landscape evolves, 2026 stands out as a turning point for cybersecurity. Artificial intelligence, quantum computing, and increasingly sophisticated threat actors are redefining how companies and individuals approach digital risks. Based on my experience as a founder and CEO in the cybersecurity sector, we will explore three major trends shaping 2026 — and what they mean for companies and users.

DPL NEWS 2026 PREDICTIONS BY COUNTRY | DIGITAL INFRASTRUCTURE AND AI: THE GEOPOLITICAL BATTLES

DPL News – The DPL News 2026 Country Predictions offer a strategic and comparative analysis of the direction the digital ecosystem will take in Latin America and the major global powers, in a context marked by geopolitical disputes surrounding digital infrastructure and Artificial Intelligence. This document goes beyond simply anticipating technological trends: it analyzes how political, regulatory, and economic decisions are defining who controls networks, computing power, data, and ultimately, digital power.

DIGI AMERICAS LATAM CISO

INSIGHTS

DECEMBER 18, 2025

CISA UPDATES CYBERSECURITY BENCHMARKS FOR CRITICAL INFRASTRUCTURE ORGANIZATIONS – USA

Utility Dive - The Cybersecurity and Infrastructure Security Agency has updated a list of goals that it hopes utilities, water treatment facilities, hospitals and other critical infrastructure operators will use to protect their systems from hackers. Version 2.0 of CISA's Cross-Sector Cybersecurity Performance Goals (CPGs), which the agency released on Thursday, "incorporates three years of operational insights, and address emerging threats through data-driven, actionable guidance," CISA said in a statement. "These enhancements are designed to promote accountability, improve risk management, and support strategic cybersecurity governance across sectors."

NIST CYBER AI PROFILE – USA

NCCOE - NIST has published the preliminary draft NIST IR 8596, Cybersecurity Artificial Intelligence Community Profile ("Cyber AI Profile"). The comment period for this publication is open through January 30, 2026. Recent advancements in Artificial Intelligence (AI) technology bring great opportunities to organizations, but also new risks and impacts that need to be managed in the domain of cybersecurity. NIST is evaluating how to use existing frameworks, such as the Cybersecurity Framework (CSF), to assist organizations as they face new or expanded risks.

TRUMP PARTNERS WITH AI FIRMS TO BUILD TECH TALENT PIPELINE – USA

Bloomberg - The Trump administration will recruit 1,000 artificial intelligence experts in the coming months through a new program aimed at modernizing the federal workforce. The effort announced Monday, called US Tech Force, aims to hire early career technologists into roles across the government — one of the administration's most tangible efforts to change the composition and culture of its workforce after shedding more than 300,000 jobs this year. The program, led by the Office of Personnel Management, will partner with more than a dozen companies—including some that have been friendly with President Donald Trump, including Palantir and Elon Musk's xAI. Other participants include OpenAI Inc., Amazon.com Inc., and Uber.

HOW THE U.S. TRADE AGREEMENT WITH MEXICO AND CANADA CAN ADVANCE CYBERSECURITY AND DEFEND CRITICAL INFRASTRUCTURE

Threat Beat - The United States-Mexico-Canada Agreement (USMCA) review is the United States' best opportunity to advance secure digital infrastructure and influence technological markets in Northern and Latin America.
On Dec. 3-5, the United States Trade Representative held a public hearing on the future of the landmark 2018 free trade accord that enumerated America's regional agenda for the first time since 1994. Across a series of panels, experts in foreign policy, trade and security made the case for the importance of digital trade – largely focusing on the importance of digital markets to America's economic growth and the need to update Section 19's digital rules to reflect current markets. However, the cybersecurity component of digital trade was seldom mentioned.