



INSIGHTS

DECEMBER 18, 2025

DIGI AMERICAS ALLIANCE MEMBERS



EMITE ATDT POLÍTICA GENERAL DE CIBERSEGURIDAD PARA LA ADMINISTRACIÓN PÚBLICA FEDERAL - MÉXICO

La Jornada - La Agencia de Transformación Digital y Telecomunicaciones emitió hoy el Acuerdo por el que se emite la Política General de Ciberseguridad para la Administración Pública Federal. En el documento difundido en el Diario Oficial de la Federación, el organismo que encabeza José Antonio Peña Merino, mencionó que la magnitud de las amenazas digitales es innegable y que según el Fortinet Global Threat Landscape Report 2025, en México se registraron más de 324 mil millones de intentos de ciberataques durante 2024, situando al país entre los más amenazados de América Latina.

MÉXICO ACELERA LA ADOPCIÓN DE INTELIGENCIA ARTIFICIAL, CIBERSEGURIDAD, TECNOLOGÍAS CUÁNTICAS Y NUBE HÍBRIDA

Comunicar - México consolida su liderazgo en innovación tecnológica en América Latina, con una adopción cada vez mayor de inteligencia artificial (IA), ciberseguridad avanzada, computación cuántica, automatización inteligente y conectividad 5G. El informe destaca que más del 60% de las empresas mexicanas está acelerando su transformación digital, impulsadas por la necesidad de aumentar la productividad, fortalecer la resiliencia operativa y responder a un entorno global altamente competitivo. Iniciativas como la Agenda Digital Nacional, la Estrategia de Ciberseguridad 2024-2030 y los programas de innovación industrial han sido factores clave en este avance.

CHILE PUBLICA EL PRIMER GRUPO DE INSTITUCIONES CALIFICADAS COMO OPERADORES DE IMPORTANCIA VITAL

Segurilatam - El Diario Oficial de la República de Chile publicó, el 17 de diciembre, la nómina de operadores de importancia vital correspondiente a los sectores eléctrico, de telecomunicaciones, servicios digitales, instituciones bancarias y financieras, prestadores de salud, empresas públicas y organismos de la Administración del Estado. De las 1.712 instituciones preliminarmente calificadas, 915 fueron declaradas por la Agencia Nacional de Ciberseguridad (ANCI) como operadores de importancia vital para la ciberseguridad del país.

SENADO APROVA MARCO LEGAL DE PROTEÇÃO DIGITAL E FORTALECE AGENDA DE CIBERSEGURANÇA PARA O MERCADO BRASILEIRO

Segs - Nova política marca avanço institucional em meio à escalada dos ataques digitais, mas especialistas alertam para o desafio de transformar diretrizes em proteção efetiva. Em um cenário em que o Brasil enfrenta milhares de tentativas de ciberataques a cada ano, o Senado Federal deu um passo estratégico ao aprovar, nesta última quarta-feira (10), a criação da Política Nacional de Proteção Digital. A medida, que segue agora para análise na Comissão de Ciência e Tecnologia (CCT), busca ampliar a resiliência do país diante de um volume de ameaças em crescimento contínuo, com impactos diretos sobre serviços públicos essenciais e cadeias críticas de infraestrutura.

EXÉRCITO PROMOVE INTEGRAÇÃO PARA DESENVOLVIMENTO DE SOLUÇÕES ESTRATÉGICAS EM CIBERSEGURANÇA - BRASIL

Defesanet - O Estado-Maior do Exército (EME), em parceria com a Escola Superior de Defesa (ESD), realizou a Oficina de Segurança Cibernética com o objetivo de identificar oportunidades, sinergias e modelos de atuação conjunta voltados ao desenvolvimento de soluções estratégicas para o ambiente digital. O encontro aproximou representantes de instituições públicas, privadas e acadêmicas, ampliando o diálogo sobre desafios e necessidades da área. Durante a oficina, especialistas apresentaram análises e experiências relacionadas à evolução das ameaças digitais, gestão de riscos e tendências em inovação tecnológica.

BRASIL LANÇA SU PRIMER MODELO DE INTELIGENCIA ARTIFICIAL ENTRENADO 100% EN PORTUGUÉS

DPL News - Brasil presentó este martes 9 de diciembre su primer modelo de Inteligencia Artificial desarrollado y entrenado íntegramente en portugués. Bautizado como **SoberanIA**, el proyecto fue lanzado durante el Encuentro Nacional de IA Soberana, en Brasilia, y reúne al Ministerio de Ciencia, Tecnología e Innovación, al gobierno del estado de Piauí, a Telebras, a la Universidad Federal de Piauí y a las empresas Modular y Scala Data Centers. Como sugiere el nombre del proyecto, la iniciativa apunta a la cuestión práctica de la soberanía digital.

DAS AMEAÇAS DA IA À SEGURANÇA QUÂNTICA: TENDÊNCIAS DE CIBERSEGURANÇA EM 2026

Forbes Brasil - À medida que o cenário digital evolui, 2026 desponta como um ponto de virada para a cibersegurança. Inteligência artificial, computação quântica e atores de ameaça cada vez mais sofisticados estão redefinindo como empresas e indivíduos encaram os riscos digitais. Com base na experiência como fundador e CEO no setor de cibersegurança, vamos explorar três grandes tendências que moldam 2026 — e o que elas significam para companhias e usuários.

PREDICCIONES DPL NEWS 2026 POR PAÍS | INFRAESTRUCTURA DIGITAL E IA: LAS BATALLAS GEOPOLÍTICAS

DPL News - Las Predicciones DPL News 2026 por país ofrecen una lectura estratégica y comparada sobre el rumbo que tomará el ecosistema digital en América Latina y las principales potencias globales, en un contexto marcado por la disputa geopolítica en torno a la infraestructura digital y la Inteligencia Artificial. Este documento no se limita a anticipar tendencias tecnológicas: analiza cómo decisiones políticas, regulatorias y económicas están definiendo quién controla las redes, el cómputo, los datos y, en última instancia, el poder digital.

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.