DIGI AMERICAS ALLIANCE MEMBERS

CHILE | SENADORES PROPONEN REGULAR USO ÉTICO DE IA EN INVESTIGACIÓN BIOMÉDICA

DPL News - Proyecto de ley busca equilibrar avance científico y protección de derechos individuales en Chile. Establece principios rectores como transparencia y no discriminación. Requiere autorización de comités de ética para investigaciones con IA. Exige supervisión humana constante en sistemas de IA. Obliga a instituciones a evaluar y mitigar riesgos, especialmente sesgos algorítmicos. Refuerza protección de datos personales y consentimiento informado. Introduce sanciones por incumplimiento.

LA CIBERSEGURIDAD COMO ASUNTO DE SEGURIDAD NACIONAL - MÉXICO

El Heraldo - La publicación del Plan Nacional de Ciberseguridad 2025–2030 representa un punto de inflexión para la seguridad nacional de México. Por primera vez, el Estado reconoce de manera explícita que el ciberespacio se ha convertido en un dominio estratégico donde convergen riesgos criminales, económicos, políticos y geopolíticos. En un entorno internacional marcado por la competencia tecnológica, la fragmentación digital y el uso del ciberespacio como instrumento de poder, este reconocimiento llega tarde, pero resulta indispensable.

MÉXICO Y ESTONIA BUSCARÁN EL INTERCAMBIO EN MATERIA DE DIGITALIZACIÓN GUBERNAMENTAL Y CIBERSEGURIDAD

Diario Noticias - Al instalarse el Grupo de Amistad México-República de Estonia, su presidenta la diputada Deliamaria González Flandez (PVEM) mencionó que este tendrá como propósito el intercambio en materia de digitalización gubernamental, ciberseguridad, capacitación tecnológica y el comercio electrónico. La legisladora indicó que la relación de ambas naciones se basa en los valores compartidos y en una visión común al futuro.

ENTRE CHIPS, DADOS E INTELIGÊNCIA ARTIFICIAL, 2025 MARCOU O AVANÇO DA SOBERANIA TECNOLÓGICA DO BRASIL

Gov.br - Quando o assunto é soberania tecnológica, 2025 foi um ano em que o Brasil decidiu acelerar o passo — e fez isso com método, investimento e visão de futuro. Sob a coordenação do Ministério da Ciência, Tecnologia e Inovação (MCTI), o país encerra o ano com R$ 267 milhões investidos em projetos estratégicos de TICs, um crescimento de 116% no fomento em relação a 2024, além de uma engrenagem institucional que passou a operar em ritmo compatível com os desafios da era digital. Em um mundo onde dados, chips, inteligência artificial e supercomputação definem poder e autonomia, o ministério transformou política pública em infraestrutura concreta para o desenvolvimento nacional.

ORÇAMENTOS DE CIBERSEGURANÇA EM 2026: PERSPECTIVAS PARA O BRASIL

Computer Weekly - Em muitos setores da economia, os orçamentos de cibersegurança em 2025 foram conservadores, mais voltados a manter as defesas já implementadas nas empresas do que inovar de fato. Relatório da Ians Research com CFOs norte-americanos de várias verticais revelou que, em média, os budgets de segurança cibernética aumentaram somente 4% em relação a 2024. Isso representa 50% da média de crescimento de 8% nesses investimentos nos últimos cinco anos. O foco foi em otimizar ao máximo os recursos que as empresas já possuíam em casa. No Brasil e na América Latina, em especial, o quadro é ainda mais complexo. Há um subinvestimento em cibersegurança que fragiliza governos e empresas, tornando a região um alvo preferencial dos criminosos.

LA MADUREZ EN CIBERSEGURIDAD MEJORA EN AMÉRICA LATINA Y EL CARIBE, SEGÚN INFORME DEL BID Y LA OEA

DPL News - Los países de América Latina y el Caribe han logrado avances significativos en el fortalecimiento de su capacidad de ciberseguridad, pero persisten diferencias en recursos, desarrollo de talento y coordinación intersectorial que continúan dejando a la región vulnerable frente a amenazas digitales en evolución, según un nuevo informe del Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA). El informe “Ciberseguridad 2025: Vulnerabilidad y desafíos de madurez para reducir brechas en América Latina y el Caribe”, elaborado en colaboración con el Global Cyber Security Capacity Centre de la Universidad de Oxford, ofrece la evaluación más completa hasta la fecha sobre la madurez en ciberseguridad en 30 países de la región. El estudio compara capacidades nacionales utilizando el Modelo de Madurez de Capacidad en Ciberseguridad para Naciones (CMM por sus siglas en inglés), lo que permite análisis comparativos en el tiempo y entre países.

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.