DIGI AMERICAS ALLIANCE MEMBERS

Apple aws Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE
fluid attacks we hack your software Google kriptos LUMU netskope paloalto NETWORKS
Resecurity Schneider Electric SISAP Sistemas Aplicativos SOPHOS tenable Trellix TrendAI

MÉXICO INSTALA PRIMER COMITÉ NACIONAL DE GESTIÓN POR COMPETENCIAS EN CIBERSEGURIDAD

eSemanal - Expertos del sector público, privado y académico establecieron el primer Comité de Gestión por Competencias en Ciberseguridad bajo el Sistema Nacional de Competencias (CONOCER). El organismo tiene como objetivo desarrollar estándares oficiales para profesionalizar el talento mediante certificaciones que funcionen como un pasaporte de habilidades para fortalecer la movilidad laboral en el canal de distribución.

PARAGUAY Y POLONIA FORTALECEN COOPERACIÓN EN SEGURIDAD Y CIBERSEGURIDAD

Mas Encarnacion - Durante el encuentro se abordaron oportunidades de cooperación entre Paraguay y Polonia en áreas clave como seguridad, ciberseguridad y amenazas híbridas, con el objetivo de fortalecer el intercambio de experiencias y la colaboración institucional entre ambos países. El ministro del Interior, Enrique Riera Escudero, encabezó una reunión con el vicecanciller de Polonia, Wojciech Zajączkowski, y su comitiva en la sede ministerial, acompañado por el viceministro de Asuntos Políticos, Oscar Campuzano. Durante el encuentro se analizaron oportunidades de cooperación bilateral en áreas estratégicas como seguridad, ciberseguridad y amenazas híbridas.

COLOMBIA: GOBIERNO PETRO PRESENTA LA HOJA DE RUTA QUE MODERNIZARÁ LA GESTIÓN DEL ESPECTRO EN COLOMBIA ENTRE 2026 Y 2029

trendTIC - En un momento decisivo para la conectividad y la adaptación digital del país, Colombia logra consolidar una nueva propuesta para administrar uno los recursos más estratégicos de su ecosistema tecnológico: la Política de Gestión de Espectro 2026-2029, liderada por el Ministerio TIC y la Agencia Nacional del Espectro (ANE). El documento, que plantea un entorno de gestión más eficiente e innovador, capaz de responder a las transformaciones de la industria, a las necesidades del Estado y a la urgencia de cerrar brechas con herramientas modernas y sostenibles, fue presentado por la ministra TIC, Carina Murcia, en Andina Link 2026, que se lleva a cabo en Cartagena.

DIGI AMERICAS LATAM CISO

INSIGHTS

MARCH 12, 2026

CABLE SUBMARINO CHILE-CHINA ABRE DEBATE SOBRE SOBERANÍA DIGITAL Y SEGURIDAD DE DATOS

Portal Innova - El proyecto de cable submarino que busca conectar directamente a Chile con Asia, y particularmente con China, reactivó un debate estratégico sobre la seguridad de los datos que circularán por esta infraestructura crítica. Aunque la discusión pública está centrada en la fibra óptica instalada en el fondo del océano, especialistas en ciberseguridad advierten que el verdadero punto sensible está en los sistemas de software que administran y gestionan el tráfico de comunicaciones. La iniciativa forma parte de los esfuerzos por fortalecer la conectividad digital de Chile y consolidar su posición como hub tecnológico en América Latina, reduciendo la dependencia de rutas que actualmente pasan principalmente por Estados Unidos. Pero, especialistas plantean que la discusión no debe limitarse a la infraestructura física, sino también considerar quién controla las plataformas tecnológicas que operan la red.

REGULAÇÃO DE IA NO BRASIL ENTRA EM DISPUTA POLÍTICA NA CÂMARA

Economic News Brasil - A regulação de IA no Brasil voltou ao centro da agenda legislativa nesta segunda-feira (09/03), após o tema ser incluído entre as prioridades da Câmara dos Deputados. O projeto que estabelece regras para o uso da inteligência artificial ainda enfrenta divergências dentro do governo federal e pressão de empresas de tecnologia, enquanto o relator, deputado Aguinaldo Ribeiro (PP-PB), prepara a apresentação de seu relatório. O texto chegou à Câmara no início de 2025 e segue sem divulgação pública. Mesmo assim, Ribeiro afirmou que pretende levar a proposta para votação na comissão especial em abril. O debate envolve a definição de limites para sistemas de inteligência artificial, a proteção de direitos fundamentais e o estímulo ao desenvolvimento tecnológico no país.

CIOS PRIORIZAM CIBERSEGURANÇA E GESTÃO DE DADOS NOS INVESTIMENTOS PARA 2026 - BRASIL

itforum - Ao mesmo tempo em que as empresas ampliam a adoção da inteligência artificial (IA) para aumentar eficiência e produtividade, também ampliam sua superfície de ataque, criando oportunidades para invasores. Sem uma infraestrutura resiliente e governança digital, a IA deixa de ser um motor de inovação e passa a ser um alvo estratégico para ataques cibernéticos e manipulações. Os CIOs brasileiros estão cientes desse desafio. Uma gestão de dados eficaz, que envolve coleta, armazenamento, classificação e descarte seguro, fornece a base necessária para que a cibersegurança implemente proteções mais precisas, evitando vazamentos e garantindo conformidade com normas como a LGPD.

ENTRE A PROTEÇÃO INTEGRAL, A GOVERNANÇA RESPONSIVA E A EDUCAÇÃO DIGITAL - BRASIL

Diplomatique Brasil - Em meio a um debate contemporâneo sobre os desafios da proteção de crianças e adolescentes no ambiente digital, ganha relevância a promulgação do chamado ECA Digital (Lei nº 15.211/2025), cuja entrada em vigor está prevista para 18 de março. Propõe-se aqui uma leitura dessa legislação a partir de três eixos: proteção integral, governança regulatória responsiva e educação digital. Mais do que descrever a norma, interessa compreender o que sua criação e implementação revelam sobre o estágio da regulação brasileira diante de um ambiente marcado por assimetrias informacionais, modelos de negócio baseados em dados e sistemas algorítmicos orientados à captura de atenção.

DIGI AMERICAS LATAM CISO

INSIGHTS

MARCH 12, 2026

AUMENTO DE FALLAS EN INTELIGENCIA ARTIFICIAL ALERTA LA CIBERSEGURIDAD GLOBAL, DICE INFORME

Nanche Michoacan - El número de fallas relacionadas con la IA podría superar los 3 mil casos en 2026, lo que se convertiría en uno de los principales riesgos de ciberseguridad. Ciudad de México. La adopción acelerada de la inteligencia artificial (IA) está generando desafíos críticos en la ciberseguridad global, según el informe 'Fault Lines in the AI Ecosystem' elaborado por TrendAI, con un alza de casi el 35 % en 2025 respecto al año anterior. Este documento reveló que en 2025 se registraron 2,130 vulnerabilidades vinculadas a la IA, un incremento del 34,6 % respecto al año anterior, lo que representa un 4,42 % de todas las fallas de software detectadas a nivel global. El análisis advirtió que, si la tendencia continúa, el número de fallas relacionadas con la inteligencia artificial podría oscilar entre 2,800 y 3,600 casos en 2026, lo que la consolidaría como uno de los principales riesgos dentro del panorama global de ciberseguridad.

WHITE HOUSE UNVEILS CYBER STRATEGY TO STRENGTHEN WORKFORCE AND NATIONAL SECURITY - USA

The Cyber Edge - The new Cyber Strategy for America, released on March 6 by the White House, outlines an approach to cybersecurity that emphasizes a proactive and unified stance across federal, state, local, tribal and private sector partners. The strategy also signals an emphasis on workforce development, including plans for a cyber academy to train the next generation of cybersecurity professionals. White House National Cyber Director Sean Cairncross described the strategy as a road map to better align federal resources and interagency actions and deepen collaboration with industry, state and local partners to counter evolving cyber threats.

WHITE HOUSE ISSUES EXECUTIVE ORDER ADDRESSING CYBERCRIME BY THREAT GROUPS - USA

American Hospital Association - The White House issued an executive order March 6 to combat cybercrimes by threat groups. The order highlights how such groups can receive willing or tacit state support for cyberattacks involving ransomware and malware, phishing, financial fraud and other schemes. The order directs federal agencies within 120 days to create an action plan that would be carried out by the National Coordination Center to identify criminal organizations “responsible for scam centers and cybercrime” and to propose solutions to dismantle those groups. The plan would describe how the attorney general and the secretary of Homeland Security should use technological capabilities, threat intelligence and operational insights from cybersecurity firms and other non-federal entities to improve attribution, tracking and disruption of cybercriminal activity. The plan would also include mechanisms to improve information sharing, operational coordination and rapid response across the federal government.

CYBERSECURITY IN CONNECTED MEDICAL DEVICES: A POLICY AGENDA FOR THE NHS - USA

Nature - Connected Medical Devices (CMD) are redefining care within the NHS but exposing it to bi-directional cyber-physical threats that traverse physical, network and cloud layers. These vulnerabilities blur the boundary between technology and patient safety. This Comment argues that the MHRA should elevate cybersecurity to a clinical-safety mandate, enforcing a unified socio-technical framework with security-by-design, cross-layer risk assessment and continuous post-market vigilance.