DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 6, 2026

DIGI AMERICAS ALLIANCE MEMBERS

MÉXICO RECONFIGURA SU GOBERNANZA DE DATOS EN MEDIO DEL VACÍO REGULATORIO DE LA IA

El Economista - Tras la extinción del INAI y el traslado de funciones al Ejecutivo, México discute estándares, auditorías y evaluaciones de impacto para sistemas de IA de alto riesgo, en un entorno donde modelos ya influyen en decisiones automatizadas sin obligaciones claras de transparencia o explicación. La protección de datos entró a una etapa de reacomodo institucional en México mientras la inteligencia artificial se integra a procesos cotidianos de trabajo, con riesgos que cruzan privacidad, seguridad, identidad y confianza en transacciones digitales, de acuerdo con especialistas que participaron en el I Foro Internacional de Protección de Datos Personales, organizado por la Academia Mexicana de Ciberseguridad y Derecho Digital (AMCID).

CON 10 CABLES SUBMARINOS, COLOMBIA SE POSICIONA COMO PUERTA DE ENTRADA DIGITAL A SUDAMÉRICA

La Nota Economica - Actualmente, Colombia cuenta con 10 cables submarinos, lo que representa una fortaleza clave para el desarrollo del sector de data centers y tecnología de datos. Esta infraestructura permite alta disponibilidad, redundancia, baja latencia y mayor resiliencia en las comunicaciones, condiciones indispensables para la operación de centros de datos de clase mundial. Gracias a su ubicación geográfica y a esta red de cables submarinos, Colombia se consolida como una puerta de entrada a Sudamérica, conectando de manera eficiente con Norteamérica, Centroamérica y otros continentes. Esta ventaja no solo facilita el tránsito de datos a gran escala, sino que convierte al país en un punto estratégico para la instalación de data centers que buscan atender mercados regionales e internacionales.

NOVA NORMA INSTITUI CRIPTOGRAFIA QUÂNTICA NO GOV.BR E EM CERTIFICADOS DIGITAIS - BRASIL

FENATI - Criptografia quântica – O Instituto Nacional de Tecnologia da Informação (ITI) iniciou a modernização da infraestrutura de certificação digital do país para se adaptar aos avanços da computação quântica. Uma Instrução Normativa publicada esta semana estabelece a adoção de algoritmos criptográficos pós-quânticos na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 6, 2026

EL SALVADOR ENFRENTA ATAQUES INFORMÁTICOS GLOBALES: POR QUÉ LA CIBERSEGURIDAD ES EL NUEVO PILAR DEL DESARROLLO NACIONAL

Infobae - La mayoría de los incidentes se originan fuera del territorio, superando controles legales nacionales; expertos advierten que el fortalecimiento de regulaciones y la conciencia sobre la huella digital son claves para el futuro económico y social. El crecimiento del cibercrimen y la sofisticación de los ataques digitales ocupan hoy el centro de la preocupación en la sociedad salvadoreña. Los expertos señalaron que los fraudes informáticos no solo han aumentado en cantidad, sino en complejidad y alcance, afectando tanto a empresas como a personas naturales.

CIBERSEGURIDAD Y TRAZABILIDAD: EL DESAFÍO QUE ESTÁ REDEFINIENDO LA SEGURIDAD LOGÍSTICA EN CHILE

Portal Innova - En un contexto de crecientes amenazas digitales y mayores exigencias regulatorias, la seguridad de la cadena de suministro se ha vuelto crítica para el comercio exterior chileno. La certificación ISO 28000 se consolida como un estándar clave para fortalecer trazabilidad, continuidad operativa y ciberseguridad en el sector extraportuario. Febrero, 2026. El aumento de amenazas digitales, las interrupciones operativas vinculadas a organizaciones criminales y el endurecimiento de las normativas han elevado la seguridad logística a un nivel estratégico en Chile. Para compañías que operan infraestructura crítica el desafío ya no se limita a proteger la carga, sino a garantizar trazabilidad, continuidad y ciberseguridad en todo el flujo operativo.

ECUADOR PRESENTA SU POLÍTICA PÚBLICA PARA EL DESARROLLO ÉTICO DE LA IA

dpl News - Ecuador presentó oficialmente la Estrategia para el Fomento del Desarrollo y Uso Ético y Responsable de la Inteligencia Artificial, un instrumento en el que el Gobierno venía trabajando desde agosto del año pasado y que pretende establecer una política pública para ordenar, guiar y acelerar la adopción de esta tecnología en el país, bajo un enfoque que prioriza la protección de derechos fundamentales, la inclusión social y la sostenibilidad ambiental. La estrategia, emitida por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MinTEL) y publicada en el Registro Oficial en enero de 2026, incorpora una una visión de implementación a cuatro años (2025–2029) y se centra en el desarrollo y uso de la Inteligencia Artificial (IA) para contribuir al bienestar social.

CIBERSEGURIDAD 2026: TENDENCIAS Y POR QUÉ IMPORTA AL NEGOCIO

El Heraldo - El 2026 marca un punto de madurez para la ciberseguridad, este año se trata solo de sumar tecnología al mismo tiempo que se transforma la forma en que las organizaciones entienden, gestionan y asumen el riesgo. La innovación, el uso extendido de inteligencia artificial y la interconexión entre ecosistemas digitales están redefiniendo cómo se crea valor y cómo se protege. El Global Cybersecurity Outlook 2026 del World Economic Forum (WEF) describe un escenario impulsado por tres pilares: el aumento constante de las amenazas, la fragmentación geopolítica que dificulta la cooperación internacional y una brecha tecnológica persistente entre organizaciones. En medio de esto, la inteligencia artificial actúa como un habilitador transversal. Aumenta productividad y automatización defensiva, pero también abre nuevos vectores de ataque y riesgos difíciles de anticipar.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 6, 2026

LATAM-GPT: LA PRIMERA INTELIGENCIA ARTIFICIAL CON IDENTIDAD LATINOAMERICANA

24 Horas - El próximo martes 10 de febrero se realizará el lanzamiento oficial de Latam-GPT, el primer Gran Modelo de Lenguaje (LLM) abierto diseñado íntegramente desde y para América Latina y el Caribe. Este hito tecnológico representa el proyecto de Inteligencia Artificial colaborativo más ambicioso de la región, y posiciona a los países del continente además de usuarios, como desarrolladores activos de tecnología de vanguardia. Latam-GPT nace como un bien público orientado a democratizar el acceso a la infraestructura habilitante necesaria para la competitividad regional, y su importancia radica en la urgencia de alcanzar una soberanía tecnológica y cultural en un contexto donde la Inteligencia Artificial está redefiniendo los márgenes de productividad mundial.

CISA ORDERS FEDERAL AGENCIES TO STRENGTHEN EDGE DEVICE SECURITY AMID RISING CYBER THREATS - USA

CISA.gov - The Cybersecurity and Infrastructure Security Agency (CISA) today issued Binding Operational Directive 26-02, Mitigating Risk From End-of-Support Edge Devices. The directive requires Federal Civilian Executive Branch (FCEB) agencies to take specific actions to drive down technical debt and minimize the risk of compromise. Within a specified timeframe, FCEB agencies must strengthen asset lifecycle management for active edge devices and remove any hardware and software devices that is no longer supported by its original equipment manufacturer. Persistent cyber threat actors are increasingly exploiting unsupported edge devices - hardware and software that no longer receive vendor updates to firmware or other security patches. Positioned at the network perimeter, these devices are especially vulnerable to persistent cyber threat actors exploiting a new or known vulnerability. To mitigate this threat, CISA is requiring FCEB agencies to adhere to standard lifecycle management processes and mandatory actions within the required time limit in this directive.

FCC ISSUES CYBERSECURITY BEST PRACTICES FOR DEFENDING AGAINST RANSOMWARE ATTACKS - USA

DWT - The Federal Communications Commission's (FCC) Public Safety and Homeland Security Bureau (Bureau) recently released a public notice (Notice) emphasizing the threat of ransomware to communications networks and urging providers to adopt various cybersecurity best practices. The Notice, dated January 29, 2026, is geared toward small-to-medium sized providers, but its recommendations are relevant to larger providers as well. The Bureau's guidance underscores that providers of all sizes, including those with potentially more limited technical and financial resources, have been targeted by ransomware actors and have faced significant operational disruption, data loss, and public safety impacts as a result.

NATIONAL CYBERSECURITY STRATEGIES DEPEND ON PUBLIC-PRIVATE TRUST, REPORT WARNS

Cybersecurity Dive - Governments should work closely with the private sector when designing and detailing their national cybersecurity strategies, a prominent think tank said in a report published on Monday. “Active participation from the private sector, particularly large technology, telecommunications, and cybersecurity firms, is critical throughout the strategy’s development,” the Center for Cybersecurity Policy and Law (CCPL) said in its white paper. “The private sector can help not only support but also deliver on the government’s cybersecurity objectives and is key to a secure and resilient nation.”