DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 12, 2026

DIGI AMERICAS ALLIANCE MEMBERS

ASAMBLEA APRUEBA PROYECTO DE LEY PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD - ECUADOR

AsambleaNacional.gob.ec - El Pleno de la Asamblea, este martes, 10 de febrero, con 82 votos afirmativos, aprobó el proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, que crea una arquitectura moderna, técnicamente fundada y constitucionalmente compatible para robustecer la ciberseguridad nacional, articular un modelo coherente de gobernanza digital, proteger infraestructura crítica y garantizar continuidad de servicios esenciales.

EL GOBIERNO LANZÓ EL CENTRO NACIONAL DE CIBERSEGURIDAD Y NOMBRÓ A SUS AUTORIDADES - ARGENTINA

Filo.news - El Gobierno oficializó la creación del Centro Nacional de Ciberseguridad (CNC), un nuevo organismo estatal encargado de resguardar los activos digitales del Estado y los sistemas vinculados a servicios públicos esenciales. La medida se estableció a través del Decreto 941/2025 y se enmarca en la modificación de la ley de Inteligencia. El CNC dependerá de la Secretaría de Innovación, Ciencia y Tecnología de la Jefatura de Gabinete y tendrá a su cargo la protección de infraestructuras críticas de información, así como la prevención y respuesta ante delitos informáticos que puedan comprometer archivos sensibles o redes estratégicas. A cargo del organismo fue designado Ariel Waissbein.

LANZAMOS LATAM-GPT: LA PRIMERA INTELIGENCIA ARTIFICIAL CREADA PARA LATINOAMÉRICA Y EL CARIBE - CHILE

Gob.cl - Chile se posiciona nuevamente a la vanguardia tecnológica regional gracias al lanzamiento de Latam-GPT, el primer gran modelo de lenguaje abierto diseñado específicamente para América Latina y el Caribe, ceremonia encabezada por el Presidente Boric. Latam GPT busca construir capacidades propias en inteligencia artificial generativa, promoviendo una gobernanza ética y una arquitectura abierta que respete nuestra cultura y contextos locales.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 12, 2026

COLOMBIA: NUEVA ALIANZA CON CHILE IMPULSARÁ LA INTELIGENCIA ARTIFICIAL Y LA SUPERCOMPUTACIÓN EN LATINOAMÉRICA

trendTIC - Colombia y Chile consolidan una alianza estratégica en Ciencia, Tecnología e Innovación con énfasis en inteligencia artificial y supercomputación, con la firma protocolaria de un Memorando de Entendimiento entre el Ministerio TIC y el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación de la nación austral. Esta articulación busca avanzar hacia la soberanía tecnológica y el fortalecimiento de capacidades digitales en la región. Con el acuerdo,

SECTOR PÚBLICO MEXICANO ENFRENTA FILTRACIONES, RANSOMWARE Y CREDENCIALES COMPROMETIDAS

El Economista - Enero de 2026 dejó al sector público en México expuesto a un patrón repetido el riesgo ya no se explica solo por un hackeo, entendido como explotación técnica sofisticada, sino por una mezcla de sistemas heredados, operación tercerizada, administración débil de identidades y una cultura de contraseñas que vuelve probable el robo de cuentas. En esa combinación, el daño no siempre ocurre en la infraestructura central, sino en los bordes del Estado digital, en aplicaciones viejas que siguen vivas, accesos que permanecen habilitados y repositorios expuestos que pueden ser descargados en bloque.

COMANDO DE DEFESA CIBERNÉTICA APRESENTA ATUAÇÃO ESTRATÉGICA DURANTE VISITA INSTITUCIONAL

Exercito Brasileiro - O Comando de Defesa Cibernética (ComDCiber) é o órgão central do Sistema Militar de Defesa Cibernética (SMDC) e integra a estrutura do Exército Brasileiro, sendo responsável por planejar, coordenar e conduzir ações de Defesa Cibernética. Sua atuação tem como foco a proteção de infraestruturas críticas, sistemas de informação e ativos estratégicos do País. Durante o encontro, os integrantes do Poder Judiciário tiveram a oportunidade de conhecer a relevância da Defesa Cibernética para a segurança nacional, especialmente no que se refere à proteção de sistemas, informações estratégicas e à garantia do uso seguro, confiável e eficaz do espaço cibernético.

AMÉRICA LATINA EN ALERTA: CASI EL 38% DE CIBERAMENAZAS GLOBALES OPERA SIN SER DETECTADA

Forbes Centroamerica - “El mayor riesgo hoy no es el ataque que genera alertas, sino el que logra pasar desapercibido”, advirtió Ricardo Villadiego, fundador y CEO de Lumu Technologies, al subrayar que una parte creciente de las intrusiones actuales consigue evadir los controles preventivos y mantenerse activa durante largos periodos sin ser identificada. El informe precisa que el 18,9% de las detecciones corresponde a ‘comportamientos maliciosos’ activos mientras que el 18,7% se vincula a dominios de ‘phishing’ en operación. Estas dos categorías reflejan actividades que van más allá de intentos bloqueados en el perímetro, afectando directamente los entornos internos de las organizaciones.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 12, 2026

CHINESE CYBERSPIES BREACH SINGAPORE'S FOUR LARGEST TELCOS

Bleeping Computer - The Chinese threat actor tracked as UNC3886 breached Singapore's four largest telecommunication service providers, Singtel, StarHub, M1, and Simba, at least once last year. The hackers also gained limited access to critical systems but did not pivot deep enough to disrupt services. In response to the intrusions, which were disclosed in July 2025, Singapore deployed 'Operation Cyber Guardian' to limit the adversary's activity on the telco's networks, but very few details were shared at the time. "Over the past months, our investigations have indicated that UNC3886 had launched a deliberate, targeted, and well-planned campaign against Singapore's telecommunications sector," Singapore's Cyber Security Agency (CSA) states.

GLOBAL CYBERSECURITY OUTLOOK 2026 REGIONAL ANALYSES

World Economic Forum - Cybersecurity risk in 2026 is accelerating, driven by rapid advances in artificial intelligence, deepening geopolitical fragmentation and increasingly complex supply chains. These regional analyses build on the Global Cybersecurity Outlook 2026 to explore how these global dynamics are unfolding across different parts of the world, offering a focused view of each region's evolving cybersecurity landscape.

CLOSING THE CYBER EQUITY GAP: HOW COLLECTIVE INVESTMENT CAN SECURE THE INTERNET FOR EVERYONE

World Economic Forum - Cybercrime is often seen as a tug-of-war: criminals innovating to stay ahead of countermeasures, while governments work to hold criminals accountable. The private sector tends to sit in the middle, trying to maximize profit while protecting customers and complying with law enforcement. Nonprofit organizations, however, also have a quiet but essential role in keeping the internet secure. For example, standards bodies develop the technical protocols that allow networks to interoperate safely. Open-source projects maintain critical cybersecurity tools. Infrastructure nonprofits safeguard the naming, numbering and routing systems that underpin the internet's functionality.

HACKTIVISTS, STATE ACTORS, CYBERCRIMINALS TARGET GLOBAL DEFENSE INDUSTRY, GOOGLE WARNS

Security Week - Google warns of escalating, multifaceted cyber threats targeting the global DIB, including contractors, suppliers, and personnel supporting military capabilities. The analysis highlights a "relentless barrage" of cyber operations from state-sponsored actors linked to China, Russia, Iran, and North Korea; pro-Russia and pro-Iran hacktivists; and cybercriminals, particularly groups launching ransomware attacks on manufacturing. China-nexus cyberespionage dominates in volume, often exploiting edge devices and zero-days for long-dwell intrusions into aerospace and defense entities. Groups conducting such operations include UNC4841, UNC3886 (blamed for the recent Singapore telecom attacks), and UNC5221.

HOW RANSOMWARE HACKERS CHOOSE THEIR VICTIMS

Cybersecurity Insiders - Ransomware attacks have become one of the most profitable forms of cyber-crime. Instead of randomly infecting computers, modern ransomware groups operate like businesses. They carefully select their targets to maximize profit while minimizing risk. Understanding how these hackers choose victims reveals why certain organizations are repeatedly attacked.