DIGI AMERICAS LATAM CISO

INSIGHTS

DECEMBER 11, 2025

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 · Strike · Telefónica · tenable · Trellix · TREND MICRO

MÉXICO PRESENTA SU PRIMER PLAN NACIONAL DE CIBERSEGURIDAD Y VA POR UNA LEY GENERAL

Wired - México busca dejar de ser reactivo para volverse preventivo en el terreno digital. La Agencia de Transformación Digital y Telecomunicaciones (ATDT) presentó este jueves el Plan Nacional de Ciberseguridad, la primera política de Estado diseñada específicamente para homologar la defensa de la infraestructura crítica y los sistemas gubernamentales. El objetivo es reducir la superficie de ataque y establecer, por fin, una "ciberresiliencia" real en la región. No se trata solo de buenas intenciones; el plan incluye la creación de una Ley General de Ciberseguridad y medidas obligatorias que se publicarán este mismo año.

‘DATA CENTERS’ EN MÉXICO: MODERNIDAD, RIESGOS Y EL ROL ESTRATÉGICO DE LA SEGURIDAD ELECTRÓNICA

Segurilatam - El crecimiento acelerado de los centros de datos (data centers) en México está redefiniendo las necesidades de seguridad física y tecnológica en la industria. Entre 2025 y 2030, se estima que la inversión en infraestructura de data centers alcance los 18.000 millones de dólares, lo que representa una expansión sin precedentes y una capacidad adicional superior a los 1.500 MW en operación. Esta evolución, impulsada por la nube, el almacenamiento masivo y la creciente demanda de inteligencia artificial, convierte a los data centers en verdaderas infraestructuras críticas del país.

GOVERNO ENVIA AO CONGRESSO PROJETO DE LEI QUE CRIA O SISTEMA NACIONAL DE INTELIGÊNCIA ARTIFICIAL - BRASIL

Capital Digital - O presidente da República, Luiz Inácio Lula da Silva, encaminhou ao Congresso Nacional, nesta noite de segunda-feira (08), em edição extra, a Mensagem número 1845 de 8 de dezembro de 2025 com o texto do Projeto de Lei que institui o “Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial”. O envio marca mais um movimento do governo federal para estruturar uma política pública abrangente destinada a organizar a expansão do ecossistema de IA no país em meio ao avanço acelerado dessa tecnologia nos setores produtivos, na administração pública e nos serviços essenciais.

DIGI AMERICAS LATAM CISO

INSIGHTS

DECEMBER 11, 2025

SENADO AVANÇA EM POLÍTICA NACIONAL DE PROTEÇÃO DIGITAL PARA SERVIÇOS PÚBLICOS - BRASIL

Senado - A criação de uma política nacional para proteger dados públicos e manter serviços essenciais em funcionamento em caso de ataques digitais deu mais um passo no Senado. A Comissão de Constituição e Justiça (CCJ) aprovou nesta quarta-feira (10) o projeto que institui o marco legal da cibersegurança e o Programa Nacional de Segurança e Resiliência Digital. O PL 4.752/2025, do senador Esperidião Amin (PP-SC), recebeu parecer favorável do senador Hamilton Mourão (Republicanos-RS) e seguirá para análise final da Comissão de Ciência e Tecnologia (CCT).

BOLIVIA Y ESPAÑA CONSOLIDAN AGENDA DE COOPERACIÓN BILATERAL EN SEGURIDAD

eju.tv - España se comprometió a brindar asesoramiento técnico, impulsar la instalación de centros de datos y compartir tecnología policial desarrollada junto a otras fuerzas iberoamericanas.El paso lo concretaron el secretario General de la Vicepresidencia de Bolivia, Iván Montoya, y el director General de la Policía Nacional de España, Francisco Pardo, durante un encuentro en la sede central de la institución policial española. Durante la reunión, las autoridades coincidieron en que el crimen organizado y la delincuencia transnacional requieren respuestas conjuntas, destacando la vigencia del convenio de cooperación vigente entre ambos países.

SEIS TENDENCIAS QUE MARCARÁN LA CIBERSEGURIDAD EN LA ERA DE LA IA EN 2026

Forbes - 2026 será el "Año del Defensor", donde la defensa autónoma de IA será la única forma de combatir los ataques de identidad impulsados por IA, el envenenamiento de datos y los riesgos cuánticos. Palo Alto Networks (NASDAQ: PANW), publicó “6 predicciones para la economía de la IA: las nuevas reglas de ciberseguridad de 2026“, pronosticando un salto transformador hacia la economía de la IA. Este nuevo modelo económico global nativo de la IA, donde la IA impulsa la productividad y las operaciones, también introduce un cambio sísmico en el riesgo.

IA AGÉNTICA ES LA NUEVA FRONTERA PARA IMPULSAR LA PRODUCTIVIDAD EN AMÉRICA LATINA: AWS

DPL News - Amazon Web Services (AWS), calificó a la Inteligencia Artificial Agéntica como la “nueva frontera” y una nueva oportunidad para la región de trabajar en los desafíos locales a través de la innovación. Para aprovechar esta oportunidad es que la compañía ha acelerado sus inversiones en la región, incluyendo los 5,000 millones de dólares para el despliegue de una región en México y el próximo lanzamiento de una nueva región en Chile en 2026. AWS proyecta que la IA Agéntica se integrará en 33% de las aplicaciones empresariales para 2028 e influirá en 15% de las decisiones comerciales diarias.

OPPORTUNISTIC PRO-RUSSIA HACKTIVISTS ATTACK US AND GLOBAL CRITICAL INFRASTRUCTURE

CISA - CISA, in partnership with Federal Bureau of Investigation, the National Security Agency, Department of Energy, Environmental Protection Agency, the Department of Defense Cyber Crime Center, and other international partners published a joint cybersecurity advisory, Pro-Russia Hacktivists Create Opportunistic Attacks Against US and Global Critical Infrastructure. This advisory, published as an addition to the joint fact sheet on Primary Mitigations to Reduce Cyber Threats to Operational Technology (OT) released in May 2025, details that pro-Russia hacktivist groups are conducting less sophisticated, lower-impact attacks against critical infrastructure entities, compared to advanced persistent threat groups.

DIGI AMERICAS LATAM CISO

INSIGHTS

DECEMBER 11, 2025

KEY CYBERSECURITY TAKEAWAYS FROM THE 2026 NDAA - USA

CSO - On Dec. 7, the House and Senate Homeland Security Committees released their compromise version of the 2026 National Defense and Authorization Act (NDAA), a nearly 3,100-page piece of legislation that contains a host of provisions to fund several Department of Defense cybersecurity efforts in fiscal year 2026. Although cybersecurity is referenced hundreds of times across the NDAA, the legislation contains provisions that, once the law becomes effective, will mark significant shifts in how the US military manages major cybersecurity tasks, particularly in the timely arena of protecting mobile communications of top brass and AI deployments, as well as more understated, but potentially high-impact, infosec duties.

CYBER THREATS TO THE U.S.: WHAT POLICYMAKERS NEED TO KNOW FOR 2026

Check Point - Cyber attacks against the United States are no longer isolated events or technical headaches. They are now powerful tools of national strategy used by foreign governments, criminal networks, and ideological groups. A new report explains how these attacks have changed from simple hacks into coordinated campaigns aimed at shaping global politics, weakening U.S. institutions, and putting pressure on American decision-makers.
This blog highlights the key takeaways for leaders responsible for national security, public policy, and critical infrastructure resilience.

NUCLEAR CYBERSECURITY RESEARCHERS AND INDUSTRY UNITE TO PROTECT NEXT-GEN REACTORS

INL - As the United States accelerates deployment of advanced and small modular reactors (A/SMRs), the nuclear energy sector is embracing a digital future. While digital systems provide operators with big benefits, they can also create vulnerabilities that enable criminals to access critical infrastructure. To protect the next generation of reactors, cybersecurity has become a critical pillar of trust, safety and resilient operations. “Cybersecurity can’t be an afterthought — it needs to be discussed and implemented now,” said J’Tia Hart, the Nuclear Nonproliferation division director at the Idaho National Laboratory (INL).

APPLE, GOOGLE SEND NEW ROUND OF CYBER THREAT NOTIFICATIONS TO USERS AROUND WORLD

Reuters - Apple (AAPL.O), opens new tab and Google have sent a new round of cyber threat notifications to users around the world, the companies said this week, announcing their latest effort to insulate customers against surveillance threats. Apple and the Alphabet-owned (GOOGL.O), opens new tab Google are two of several tech companies that regularly issue warnings to users when they determine they may have been targeted by state-backed hackers. Apple said the warnings were issued on Dec. 2 but gave few further details about the alleged hacking activity and did not address questions about the number of users targeted or say who was thought to be conducting the surveillance. Apple said that "to date we have notified users in over 150 countries in total."
Apple's statement follows Google's Dec. 3 announcement, opens new tab that it was warning all known users targeted using Intellexa spyware, which it said spanned "several hundred accounts across various countries, including Pakistan, Kazakhstan, Angola, Egypt, Uzbekistan, Saudi Arabia, and Tajikistan."