DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 20, 2026

DIGI AMERICAS ALLIANCE MEMBERS

NUEVA LEY DE TELECOMUNICACIONES DE REPÚBLICA DOMINICANA REGULARÁ REDES, NO PLATAFORMAS

DPL News - A dos años de haberlo anunciado, el Instituto Dominicano de las Telecomunicaciones (Indotel) presentó la propuesta de Ley General de Telecomunicaciones, Infraestructura Digital y Conectividad, con la que busca actualizar el marco jurídico del sector y responder a los desafíos de la transformación tecnológica. La iniciativa retoma la Ley 153-98 e incorpora herramientas más modernas, acordes con la convergencia de la fibra óptica, las nuevas generaciones móviles, las comunicaciones satelitales, los cables submarinos y los centros de datos. La propuesta establece que la regulación se concentrará en las redes, servicios e infraestructuras vinculados a las telecomunicaciones, sin regular contenidos, comercio electrónico ni plataformas digitales, e incorpora un régimen sectorial de ciberseguridad orientado a fortalecer la integridad, continuidad y resiliencia de la infraestructura digital.

LEY DE CIBERSEGURIDAD DE GUATEMALA PODRÍA ESTAR LISTA EN NOVIEMBRE SI SUPERA DICTAMEN Y DISCUSIÓN

Prensa Libre - Guatemala no tiene un marco regulatorio aprobado en materia de ciberseguridad y protección de datos. Han pasado 17 años y el Congreso ha recibido ocho iniciativas relacionadas, sin que ninguna se haya convertido en ley, mientras el país avanza en la digitalización de servicios financieros y de energía. A esto se suma que la adhesión de Guatemala al Convenio de Budapest está condicionada a la aprobación de la iniciativa, con una prórroga del Consejo de Europa que vence en marzo de 2027.

CREAN MESA NACIONAL PARA COMBATIR EL FRAUDE FINANCIERO TRANSNACIONAL - CHILE

El Nortero - Ante el aumento de estafas cada vez más sofisticadas, instituciones públicas, privadas y académicas firmaron un convenio para constituir en Chile una Mesa Nacional contra el Fraude Financiero Transnacional. La iniciativa, liderada por el Fiscal Nacional Ángel Valencia, suma al Ministerio Público, la Agencia Nacional de Ciberseguridad (ANCI), la Comisión para el Mercado Financiero (CMF), el Servicio de Impuestos Internos, la Unidad de Análisis Financiero y el SERNAC, junto a gremios bancarios y del retail financiero y la Universidad de Chile. El objetivo es crear un marco permanente de cooperación para prevenir, detectar y perseguir de manera más eficaz los fraudes financieros, con intercambio sistemático de información y la identificación de patrones criminales operados desde plataformas internacionales.

DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 20, 2026

COSTA RICA EN SEGUNDO LUGAR REGIONAL EN RESILIENCIA CIBERNÉTICA

CR Hoy - Costa Rica se ubica como el segundo país con mayor resiliencia cibernética del Caribe y Centroamérica, con un índice del 53%, de acuerdo con el Ranking Regional de Resiliencia Cibernética de SISAP. El resultado la coloca detrás de República Dominicana, que registra un 54%, y por delante de Panamá (49%), Colombia (48%), El Salvador (41%), Guatemala (39%), Honduras (34%) y Nicaragua (32%). Los resultados reflejan diferencias en las capacidades de los países para prevenir, responder y recuperarse ante incidentes de ciberseguridad. El estudio identifica al Gobierno, los servicios financieros, la manufactura, el retail y el sector de tecnología como las industrias con mayor impacto económico potencial ante un ciberataque, con una exposición conjunta cercana a los $1.4 mil millones.

ANPD PUBLICA METODOLOGIA DE TESTAGEM DO SANDBOX REGULATÓRIO EM IA E PROTEÇÃO DE DADOS - BRASIL

gov.br - A Agência Nacional de Proteção de Dados (ANPD) publicou a metodologia de testagem do Sandbox Regulatório em Inteligência Artificial e Proteção de Dados, documento que apresenta os procedimentos de supervisão, monitoramento e avaliação das soluções dos participantes do projeto-piloto. Desenvolvida pelo Centro de Inteligência Artificial e Aprendizado de Máquina da USP e validada pela Comissão de Sandbox da Agência, a metodologia busca avaliar aspectos relacionados à transparência, explicabilidade e proteção de dados pessoais em sistemas de IA.

NACIONES UNIDAS PREVIENE CIBERDELITOS CON DIVERSAS INICIATIVAS

Reseller - Con diferentes programas, la Organización de las Naciones Unidas previene ciberdelitos que afectan tanto al sector empresarial como a la ciudadanía. El esquema integra ciberseguridad y persecución de los ciberdelitos, vinculados con la protección de la ciudadanía. Según Víctor Merchand, coordinador del Programa de Ciberdelito de la ONU en México, la organización realiza actividades de protección de datos y prevención del delito, así como el fortalecimiento de capacidades de las autoridades para identificar, investigar y perseguir el crimen. El vocero subrayó que la inteligencia artificial juega un papel central tanto en la protección como en el nivel de riesgo al que se expone la ciudadanía, y recomendó a las empresas pensar a un nivel estratégico más alto para proteger infraestructuras, economía y personas.

EXPANDING CYBER CAPABILITIES AGAINST TRANSNATIONAL CRIME - USA

Center for Cybersecurity Policy and Law - On August 12, the White House issued a Presidential Memorandum establishing a new program to authorize vetted U.S. companies to conduct cyber surveillance and cyber effects operations against certain transnational criminal organizations under federal direction, authorization, and oversight. Led by the Department of Homeland Security and the Department of Justice, the program follows Executive Order 14390 of March 2026 and builds on the March 2026 Cyber Strategy's call to unleash the private sector against adversary networks. The memorandum sets a framework for private-sector support of government operations targeting cyber-enabled transnational criminal groups, while prohibiting operations expected to result in loss of life or that rise to the level of use of force. Key legal and operational details remain to be developed within 60 days of publication.

DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 20, 2026

NSA, FBI WARN OF HACKERS USING AI-GENERATED TOOLS IN ATTACKS ON CRITICAL INFRASTRUCTURE TECHNOLOGY - USA

The Record - Federal agencies warned of an active threat targeting critical infrastructure organizations using AI-generated exploit scripts, in what they called an evolution in capabilities. The National Security Agency, FBI and other agencies said the campaign is targeting Siemens S7 Series PLCs, tools used by the energy, water and agricultural industries, and was being fueled by AI-assisted development alongside exploitation of known vulnerabilities. Threat actors are conducting reconnaissance against U.S.-based Siemens PLC installations using AI-generated exploitation scripts disguised as legitimate monitoring tools.

NSSTS STRATEGY TARGETS CYBERSECURITY, OT/ICS RESILIENCE AND TECHNOLOGY SUPPLY CHAINS, OUTLINES FOUR PILLARS - USA

Industrial Cyber - The White House released its National Security Science and Technology Strategy (NSSTS), which sets out four pillars of scientific and technological development tied to national security, with implications for cybersecurity, operational technology and industrial control system (OT/ICS) resilience, and technology supply chains. The first pillar, Focusing Techno-Strategic Competition, emphasizes maintaining U.S. technological advantage on the battlefield, highlighting undersea, space, and artificial intelligence and autonomy as priority areas, alongside countering strategic threats to the homeland.

BANCO GENERAL REFUERZA SU APUESTA POR LA CIBERSEGURIDAD ANTE EL AVANCE DE LA INTELIGENCIA ARTIFICIAL

Revista Summa - La ciberseguridad dejó de ser un asunto exclusivamente tecnológico para convertirse en un componente estratégico de la gestión empresarial. Así lo planteó Banco General durante un desayuno ejecutivo y conversatorio realizado en Costa Rica, donde líderes del sector financiero y empresarial analizaron los nuevos desafíos derivados del avance de la inteligencia artificial. La entidad informó que durante 2025 invirtió más de US$31 millones en ciberseguridad, como parte de una estrategia orientada a fortalecer su capacidad de prevención, detección y respuesta. Los especialistas advirtieron que la IA permite a los atacantes analizar información con mayor rapidez y desarrollar mecanismos de fraude más sofisticados, y coincidieron en la necesidad de establecer marcos de gobierno que permitan aprovechar la tecnología sin aumentar los riesgos.

LAS EMPRESAS CAMBIAN SU ESTRATEGIA PARA EVITAR QUE UN CIBERATAQUE SE CONVIERTA EN UNA CRISIS

Technocio - Los ciberataques siguen creciendo a un ritmo que preocupa a organizaciones de todos los sectores. Según Check Point Research, durante el primer trimestre de 2025 las empresas registraron en promedio 1.925 ciberataques por semana, un 47% más que un año atrás, mientras que en América Latina el aumento alcanzó el 108%. Frente a este escenario, las empresas están pasando de una estrategia reactiva a una basada en inteligencia, monitoreo continuo y respuesta temprana. Los Centros de Operaciones de Seguridad (SOC) se han convertido en una de las principales herramientas para mantener visibilidad permanente sobre los entornos tecnológicos, combinando inteligencia artificial, analítica avanzada y la experiencia de profesionales especializados para reducir el tiempo entre la detección de una anomalía y la respuesta.