DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 20, 2026

DIGI AMERICAS ALLIANCE MEMBERS

DOMINICAN REPUBLIC'S NEW TELECOMMUNICATIONS LAW WILL REGULATE NETWORKS, NOT PLATFORMS

DPL News – Two years after announcing it, the Dominican Telecommunications Institute (Indotel) presented its proposed General Law on Telecommunications, Digital Infrastructure, and Connectivity, which aims to update the sector's legal framework and address the challenges of technological transformation. The initiative builds upon Law 153-98 and incorporates more modern tools, in line with the convergence of fiber optics, new mobile generations, satellite communications, submarine cables, and data centers. The proposal stipulates that regulation will focus on telecommunications networks, services, and infrastructure, without regulating content, e-commerce, or digital platforms. It also incorporates a sector-specific cybersecurity regime designed to strengthen the integrity, continuity, and resilience of the digital infrastructure.

GUATEMALA'S CYBERSECURITY LAW COULD BE READY IN NOVEMBER IF IT PASSES THE INITIAL REVIEW AND DEBATE

Prensa Libre – Guatemala lacks an approved regulatory framework for cybersecurity and data protection. Seventeen years have passed, and Congress has received eight related initiatives, none of which have become law, even as the country moves forward with the digitalization of financial and energy services. Furthermore, Guatemala's accession to the Budapest Convention is contingent upon the approval of this initiative, with an extension granted by the Council of Europe that expires in March 2027.

NATIONAL TASK FORCE CREATED TO COMBAT TRANSNATIONAL FINANCIAL FRAUD - CHILE

El Nortero - In response to the rise in increasingly sophisticated scams, public, private, and academic institutions have signed an agreement to establish a National Roundtable Against Transnational Financial Fraud in Chile. The initiative, led by National Prosecutor Ángel Valencia, brings together the Public Prosecutor's Office, the National Cybersecurity Agency (ANCI), the Financial Market Commission (CMF), the Internal Revenue Service, the Financial Analysis Unit, and SERNAC (National Consumer Service), along with banking and financial retail associations and the University of Chile. The goal is to create a permanent framework for cooperation to more effectively prevent, detect, and prosecute financial fraud through the systematic exchange of information and the identification of criminal patterns operating from international platforms.

DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 20, 2026

COSTA RICA RANKS SECOND REGIONALLY IN CYBER RESILIENCE

Costa Rica Today – Costa Rica ranks as the second most resilient country in the Caribbean and Central America in terms of cybersecurity, with an index of 53%, according to the SISAP Regional Cybersecurity Resilience Ranking. This result places it behind the Dominican Republic, which registers 54%, and ahead of Panama (49%), Colombia (48%), El Salvador (41%), Guatemala (39%), Honduras (34%), and Nicaragua (32%). The results reflect differences in countries' capabilities to prevent, respond to, and recover from cybersecurity incidents. The study identifies government, financial services, manufacturing, retail, and the technology sector as the industries with the greatest potential economic impact from a cyberattack, with a combined exposure of approximately $1.4 billion.

ANPD PUBLISHES TESTING METHODOLOGY FOR THE REGULATORY SANDBOX IN AI AND DATA PROTECTION - BRAZIL

gov.br - The National Data Protection Agency (ANPD) has published the testing methodology for the Regulatory Sandbox in Artificial Intelligence and Data Protection, a document that presents the procedures for supervision, monitoring, and evaluation of the solutions from participants in the pilot project. Developed by the Center for Artificial Intelligence and Machine Learning at USP and validated by the Agency's Sandbox Committee, the methodology seeks to evaluate aspects related to transparency, explainability, and protection of personal data in AI systems.

THE UNITED NATIONS PREVENTS CYBERCRIME THROUGH VARIOUS INITIATIVES

Reseller - Through various programs, the United Nations prevents cybercrimes that affect both the business sector and citizens. The framework integrates cybersecurity and the prosecution of cybercrimes, linked to citizen protection. According to Víctor Merchand, coordinator of the UN Cybercrime Program in Mexico, the organization carries out data protection and crime prevention activities, as well as strengthening the capacities of authorities to identify, investigate, and prosecute crime. The spokesperson emphasized that artificial intelligence plays a central role in both protection and the level of risk to which citizens are exposed, and recommended that companies think at a higher strategic level to protect infrastructure, the economy, and people.

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 REINFORCES ITS COMMITMENT TO CYBERSECURITY IN THE FACE OF THE ADVANCE OF ARTIFICIAL INTELLIGENCE

Summa Magazine - Cybersecurity has ceased to be solely a technological issue and has become a strategic component of business management. This was the message conveyed by Banco General during an executive breakfast and discussion held in Costa Rica, where leaders from the financial and business sectors analyzed the new challenges arising from the advancement of artificial intelligence. The bank reported that it invested more than US$31 million in cybersecurity during 2025, as part of a strategy aimed at strengthening its prevention, detection, and response capabilities. Experts warned that AI allows attackers to analyze information more quickly and develop more sophisticated fraud mechanisms, and they agreed on the need to establish governance frameworks that allow for leveraging technology without increasing risks.

COMPANIES ARE CHANGING THEIR STRATEGY TO PREVENT A CYBERATTACK FROM TURNING INTO A CRISIS

Technocio - Cyberattacks continue to grow at a rate that worries organizations across all sectors. According to Check Point Research, during the first quarter of 2025, companies registered an average of 1,925 cyberattacks per week, 47% more than a year earlier, while in Latin America the increase reached 108%. Faced with this scenario, companies are shifting from a reactive strategy to one based on intelligence, continuous monitoring, and early response. Security Operations Centers (SOCs) have become one of the main tools for maintaining constant visibility over technological environments, combining artificial intelligence, advanced analytics, and the expertise of specialized professionals to reduce the time between anomaly detection and response.