DIGI AMERICAS LATAM CISO

# INSIGHTS

OCTOBER 16, 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

## CONNECT PLAN: INSTITUTIONS STRENGTHEN CYBERSECURITY AND CYBER DEFENSE - GUATEMALA

AGN - Guatemala City, Oct 14 (AGN) - Protecting the country's information is a strategic priority of the Conecta Plan, led by the Ministry of Communications, Infrastructure and Housing (CIV), which seeks to strengthen connectivity and the country's digital transformation. In this regard, the CIV, through the Superintendency of Telecommunications (SIT), held the Guatemala CIRT National Assessment Version 1.0 training session, focused on strengthening national cybersecurity and preparing the country for digital threats.

## ANATEL WANTS DATA CENTERS OUTSIDE THE SOUTHEAST AND STRENGTHENS REGULATION - BRAZIL

Digital Convergence - Anatel advocates for the decentralization of data centers installed in the Southeast and the expansion of this essential infrastructure to other regions of the country, as a way to reduce risks, improve connectivity, and strengthen Brazil's digital sovereignty. The recommendation is part of the White Paper "Data Centers in Brazil," which brings together technical diagnoses and regulatory proposals for the sector. The study recognizes that data centers—facilities that store and process data—are now critical infrastructure for the digital economy, supporting everything from public services to banking operations, healthcare systems, and telecommunications platforms.

## CYBERSECURITY IN FINTECHS GAINS URGENCY IN THE FACE OF ADVANCING DIGITAL THREATS - BRAZIL

Economic News Brasil - Cybersecurity in fintechs has become a priority for regulators and companies after a series of recent breaches, including the Monbank incident in September 2025, which exposed customer data and raised alarms across the financial system. The incident, in which a hacker attack embezzled R$4.9 million from the digital bank, revealed that even institutions that comply with basic rules can suffer incidents when there is no continuous monitoring of vulnerabilities.

## SÁNCHEZ ANNOUNCES THE CREATION OF A NEW NATIONAL CYBERSECURITY CENTER - SPAIN

Public - The President of the Government, Pedro Sánchez, announced this Thursday the upcoming creation of a National Cybersecurity Center. This body will be attached to the Presidency of the Government, as Sánchez himself highlighted during the closing ceremony of the 19th International Meeting on Information Security (ENISE), organized by the National Cybersecurity Institute of Spain (INCIBE) in León. The objective of this initiative is to "strengthen the coordination and strength" of the national cybersecurity system. It will join the already underway review of the National Cybersecurity Strategy of the Digital Spain Plan. The President of the Government highlighted three lines of action in this area. On the one hand, to strengthen the cybersecurity ecosystem in our country; on the other, to "promote innovation"; and, finally, to "increase investment."

## THE SPANISH NATIONAL CYBERSECURITY COUNCIL (CCN) STRENGTHENS CYBERSECURITY IN LATIN AMERICA WITH TRAINING AIMED AT 18 COUNTRIES

Segurilatam - Spain's National Cryptologic Center (CCN) has launched the third edition of the "Essential Incident Management Route" cybersecurity training program, aimed at incident response teams from 18 Latin American countries. For 28 weeks, nearly one hundred cybersecurity specialists from the CSIRTAmericas Network will receive advanced technical training through Ángeles, the CCN's cybersecurity training, capacity building, and talent platform.

## RANSOMWARE AND INDUSTRIAL ESPIONAGE: CRITICAL CHALLENGES FACING THE MANUFACTURING SECTOR - CHILE

TrendTIC - The manufacturing industry faces a complex set of risks that operate with minimal tolerance for downtime. They are also part of extensive and often complex supply chains, and their competitive advantage is often based on high-value intellectual property, such as patented designs and trade secrets. IT and security teams need to be on alert, as modern cyberattacks are sophisticated and persistent, combining technical exploits with social engineering and credential theft. They seek to remain undetected, gathering information and mapping systems before attacking.

## BOTS AND DEEPFAKES ARE DRIVING A NEW WAVE OF CYBER FRAUD: THE UTMOST IMPORTANCE FOR CYBERSECURITY COMPANIES TO COMMUNICATE ON OFFICIAL, NICHE, PRESTIGIOUS, AND INDEPENDENT SITES - CHILE

TrendTIC - The internet is entering a new era of sophistication, and so are online scams. From AI-cloned relatives demanding money to deepfake executives tricking employees into making multimillion-dollar transfers, online fraud has evolved from phishing links to synthetic identities that look and sound real. This year alone, deepfake fraud could increase by 162%, affecting both businesses and individuals.

## THE PROTECTION OF CHILDREN ON THE INTERNET AS AN ELEMENT OF DIGITAL SOVEREIGNTY

DPL News - The debate on digital regulation has ceased to be a merely technical issue and has become a central focus of global political, economic, and geopolitical discussions. Brazilian President Luiz Inácio Lula da Silva's recent address to the UN clearly demonstrates this: protecting the most vulnerable in the digital environment, especially children and adolescents, is not only a matter of human rights, but also a democratic and strategic imperative. In a context where the Internet has amplified both opportunities and risks, establishing regulatory frameworks becomes necessary, although it requires dialogue and consensus.

## OFFICIALS CRACK DOWN ON SOUTHEAST ASIA CYBERCRIME NETWORKS, SEIZE $15B

Cyberscoop - Federal authorities seized 127,271 Bitcoin, valued at approximately $15 billion, from Chen Zhi, the alleged leader of a sprawling cybercrime network based in Cambodia, the Justice Department said Tuesday. Officials said it’s the largest financial seizure on record. Officials said Chen, a 38-year-old United Kingdom and Cambodian national who has renounced his Chinese citizenship, built a business empire under the Prince Group umbrella headquartered in Phnom Penh, Cambodia, that constructs, operates and manages scam compounds that rely on human trafficking and modern-day slavery.

## CYBERCRIMINALS IMPERSONATE OPENAI AND SORA TO HARVEST USER CREDENTIALS

Cyber Press - The launch of Sora 2 AI has triggered a surge in malicious activity, as cybercriminals deploy deceptive domains impersonating OpenAI’s official services to steal user credentials and conduct large-scale crypto fraud. Multiple threat intelligence reports confirm that cloned Sora webpages are being used for credential harvesting, crypto wallet theft, and unauthorized access to paid API plans.

## CYBERSECURITY AND OTHER CRITICAL ISSUES TAKE CENTRE STAGE AS EXPERTS MEET IN DUBAI

WEF - Hundreds of experts on a wide range of critical topics converged on Dubai, United Arab Emirates, this week for the World Economic Forum’s Annual Meetings of the Global Future Councils and Cybersecurity (AMGFCC). The joint gathering between the Annual Meeting of the Global Future Councils (AMGFC) and the Annual Meeting on Cybersecurity (AMC) took place against a backdrop of jarring geopolitical shifts and advances in artificial intelligence, a hardening of multipolarity, and increased vulnerability to cyber threats and disinformation.