DIGI AMERICAS ALLIANCE MEMBERS

Apple aws Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks
Google kriptos LUMU mastercard netskope paloalto NETWORKS Resecurity Schneider Electric
SISAP Sistemas Aplicativos SOPHOS TANIUM tenable Trellix TrendAI whalemate zscaler

PANAMA AND 5G: THE CHALLENGE OF BUILDING CYBERSECURITY REGULATIONS FOR CRITICAL INFRASTRUCTURE

La Estrella de Panama – With the upcoming rollout of 5G technology, experts warn that Panama still lacks a comprehensive cybersecurity framework to protect critical infrastructure and telecommunications networks. The experience of regions such as the European Union, the United States, and Costa Rica demonstrates the importance of establishing standards that strengthen digital security, user trust, and the resilience of strategic services.

US DELIVERS MARITIME, BORDER AND CYBER SECURITY EQUIPMENT TO PANAMA

La Tribuna - The U.S. Embassy announced Wednesday that it delivered $5 million worth of essential maritime, border, and cybersecurity equipment to the Panamanian government as part of cooperation to dismantle networks that fuel irregular migration and drug trafficking and strengthen the protection of the Panama Canal. "This support is part of the expanded security cooperation between U.S. Southern Command and Panama, which is expected to reach an estimated value of $100 million by 2026," the U.S. Embassy stated in a press release.

COLOMBIAN GOVERNMENT ACTIVATES CYBER PMU TO PROTECT THE SECOND ROUND OF ELECTIONS

ImpactoTIC - With the goal of safeguarding the digital environment and strengthening public trust ahead of the presidential runoff election on June 21, the Ministry of Information and Communications Technologies (ICT) announced the activation of the Unified Cyber Command Post (PMU). The strategy aims to coordinate monitoring, prevention, and response actions against cybersecurity incidents that could affect the normal course of the democratic process. The Cyber PMU is not a new initiative. It was officially established on March 8, 2016, to support the legislative elections and has since functioned as an inter-institutional coordination mechanism among entities responsible for digital security, defense, and electoral organization.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 18, 2026

THE G7 WILL WORK TO ENSURE THAT AI MODELS DO NOT FALL INTO THE HANDS OF AUTHORITARIAN REGIMES

Infobae - The G7 has launched a joint effort to regulate advanced artificial intelligence (AI) models in order to prevent the threats they may pose to cybersecurity and society, and also to prevent them from falling into the hands of authoritarian regimes. French President Emmanuel Macron explained at the end of the G7 summit in Évian, which concluded with a luncheon between the leaders of the seven wealthiest nations and a dozen executives from technology companies, that the idea is to build, in the coming months, "a platform for discussion and cooperation among democracies to address the risks of artificial intelligence."

DRONES AND CYBERSECURITY: THE REPORT THAT WARNS THE 2026 WORLD CUP AND ITS FANS

Redgol - Security measures have been tightened at the 2026 World Cup, being held in Canada, the United States, and Mexico, raising concerns among authorities. For example, the FBI has implemented a zero-tolerance policy for drones in stadiums, prohibiting them from approaching the venues and areas where fans are gathered. Meanwhile, in Mexico, the Special Anti-Drone Group, alerted by the country's National Guard, shot down a drone that approached the training grounds of the South Korean national team, though they were unable to locate those responsible. "Before the national team arrived, two foreign men suspected of being the operators fled with the drone," they explained.

THIS IS HOW LATIN AMERICAN COUNTRIES ARE PROGRESSING WITH THE COMMITMENTS OF THE 2025 WORLD TELECOMMUNICATION CONFERENCE

dpl News – Representatives from Mexico, Guatemala, Honduras, Panama, and Trinidad and Tobago, meeting at the 2026 Regional Development Forum for the Americas (ITURDF2026), presented the actions they are implementing to continue the commitments made during the 2025 World Telecommunication Development Conference (WTDC-25). The panelists highlighted that Latin America is translating the commitments made at WTDC-25 into concrete actions related to connectivity, regulatory modernization, spectrum management, cybersecurity, and Artificial Intelligence (AI). However, challenges remain, especially in rural areas and among historically excluded populations. They also agreed on the need to coordinate efforts to accelerate digital inclusion and leverage the opportunities offered by new technologies.

BRAZIL'S MATURING MARKET MEETS MATURING THREATS: HOW GLOBAL CRYPTO CRIME TRENDS ARE LANDING IN LATIN AMERICA'S LARGEST MARKET

Chainalysis - Brazil is Latin America's largest crypto market, and one of the world's most dynamic. Between July 2024 and June 2025, the country received an estimated $318 billion in on-chain value, roughly one-third of all cryptocurrency value received across Latin America. A large, relatively young population, a vibrant fintech sector that has normalized digital financial services for millions, and persistent demand for dollar-pegged stablecoins as an inflation hedge have all fueled that growth. But when a legitimate market grows at such a pace, it draws attention from illicit actors, too. Our data shows that's exactly what's happening. The same criminal networks dominating crypto laundering activity worldwide — Chinese-language money laundering networks (CMLNs), Russian sanctions evaders, and drug traffickers — have found a significant foothold in Brazil's exchanges, according to our data.

WHITE HOUSE ROLLS OUT NSPM-12 TO BOOST CYBERSECURITY GOVERNANCE, OVERSIGHT, ACCOUNTABILITY FOR NATIONAL SECURITY SYSTEMS - USA

Industrial Cyber - The White House issued National Security Presidential Memorandum 12 (NSPM-12), establishing a new cybersecurity governance framework for National Security Systems (NSS), including military, intelligence, and other federal systems that process classified information. The memorandum re-establishes the Committee on National Security Systems (CNSS), a decades-old interagency body, designates the National Security Agency as the National Manager for NSS cybersecurity with expanded authority to assess security posture, issue emergency directives, and coordinate government-wide cyber defense activities.

OT SECURITY MATURITY IMPROVES ACROSS LATIN AMERICA

Mexico Business News - Organizations across Latin America are improving OT cybersecurity governance, visibility, and compliance readiness. However, cyber threats targeting industrial environments continue to evolve, keeping operational risk at elevated levels. The report suggests that organizations are becoming more realistic about their cybersecurity capabilities while recognizing that visibility, segmentation, remote access security, incident response, and architecture standardization remain critical areas requiring investment. This shift reflects a broader market transition in which OT security is increasingly linked to executive oversight, regulatory compliance, and operational resilience.

CYBERCRIME IS CONVERGING. THE RESPONSE MUST CONVERGE FASTER

WEF - Cybercrime is evolving into a converged criminal economy that connects online fraud, ransomware, extortion, money laundering, human trafficking, organized crime and, in some cases, state-aligned activity.
This convergence changes the nature of the threat. Criminal groups are not merely adopting new tools. They are combining capabilities, sharing infrastructure and building operating models that span technical, geographic and jurisdictional boundaries. The same ecosystem that supports credential theft or ransomware can also fund scam compounds, exploit trafficked labor, move illicit proceeds and goods and enable broader organized crime.

AI, QUANTUM AND THE NEW CYBERSECURITY FRAMEWORK IMPERATIVE

Forbes - With developing technologies, cybersecurity, and risk, one theme has been consistent: technical innovation continues to outpace our ability to safeguard it. Today's organizations face a defining problem. They must work in a world where artificial intelligence, quantum computing, cloud services, edge computing, IoT, sophisticated telecommunications, and digital ecosystems increasingly intertwine. The consequent prospects are remarkable. The risks are as significant. The cybersecurity discussion must be limited to attack prevention. The true task for this year and beyond is to strengthen organizational resilience and promote trust in an increasingly interconnected society. The digital economy now relies on trust as its currency. Customers entrust firms with their personal information. Citizens trust their governments to protect key services. Businesses rely on global supply chains, cloud providers, and digital platforms to support critical operations.