DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 12, 2025

DIGI AMERICAS ALLIANCE MEMBERS

COSTA RICA BEGAN DEVELOPING A PROPOSAL FOR A NATIONAL CYBERSECURITY INCIDENT RESPONSE PLAN

Delfino - With the goal of developing a proposal for a National Cybersecurity Incident Response Plan, last Friday the Ministry of Science, Innovation, Technology and Telecommunications (MICITT), through its Cybersecurity Directorate, received 30 officials from public institutions in our country responsible for digital security. By identifying and prioritizing critical infrastructure and establishing effective coordination mechanisms among stakeholders in the national cybersecurity ecosystem, the initiative will enable government institutions to jointly address cyber incidents in a timely, coordinated, and effective manner.

NEW PROPOSAL SEEKS TO CREATE A LEGAL FRAMEWORK TO PROTECT NATIONAL CYBERSPACE - PARAGUAY

El Nacional - Representative Federico Franco (PLRA) presented a bill entitled "On Cybersecurity and Protection of Paraguayan Cyberspace," a comprehensive initiative that seeks to establish an updated legal framework to address the growing cyber threats affecting the country. The proposal arises in response to the increasing digitalization of Paraguayan society, which has brought significant benefits but has also increased exposure to sophisticated cyberattacks capable of compromising national security, critical infrastructure, and the country's economic stability.

AMID PEÑA HACK, LAUNCH OF CYBERSECURITY STRATEGY SUSPENDED - PARAGUAY

Ultima Hora - The Ministry of Information and Communication Technologies (Mitic) has decided to postpone the launch of the National Cybersecurity Strategy 2025-2028, which was scheduled for this Tuesday at the Tiríka hall in Mburuvicha Róga. The event has not yet been scheduled for a new date, according to Mitic, and its suspension comes right in the midst of the hacking of President Santiago Peña's X account.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 12, 2025

THE IMPORTANCE OF CYBERSECURITY IN COLOMBIAN LOGISTICS

CN - In an increasingly digitalized logistics environment, traditional risks such as merchandise theft, fraud, and loss of traceability are now intertwined with a more sophisticated and growing threat: cyberattacks. In Colombia, the digital transformation of logistics companies has brought significant improvements in efficiency, but has also exposed organizations to new vulnerabilities.

INTELLIGENCE BUBBLE AND FOCUS ON CYBERSECURITY AMONG GOVERNMENT MEASURES TO ENSURE SECURITY IN THE 2026 ELECTIONS - COLOMBIA

Cambio - At the end of the meeting of the National Commission for the Coordination and Monitoring of Electoral Processes, the Minister of National Defense, Pedro Sánchez Suárez, along with the military and police leadership, made a series of announcements addressed to leaders and representatives of political parties and movements, who attended the Casa de Nariño to raise concerns, exchange ideas, and define strategies to guarantee security and tranquility during the upcoming democratic process.

74% OF GLOBAL EMPLOYERS FACE TALENT SHORTAGES; COLOMBIA PRIORITIZES AI AND CYBERSECURITY TRAINING

Identidad Latina - Rapid technological evolution, driven by artificial intelligence and automation, is transforming the global labor market, but it also creates a growing challenge: the shortage of qualified personnel. According to a global study by ManpowerGroup analyzed by Fedesoft, 74% of employers worldwide are struggling to fill vacancies with suitable professionals. In Colombia, this figure is 59% overall and reaches 68% in the technology sector.

RESPONSES TO CITIZEN COMMENTS ON THE UPDATE TO THE INFORMATION SECURITY AND PRIVACY MODEL PUBLISHED - COLOMBIA

MinTIC - The Ministry of Information and Communications Technology (MinTIC) publishes the official response to comments submitted by citizens, interest groups, and specialized entities on the draft resolution "By which Annex 1 of Resolution 500 of 2021 is updated and other related provisions are repealed."

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 12, 2025

NEURODATA IS THE NEW DIGITAL GOLD - MEXICO

Infonor - With the advent of neurotechnologies that promise to help combat depression or implant chips in the brain to connect them to computers, we must be aware of the need to protect our biometric data (which includes brain waves) to prevent misuse.

THE EUROPEAN UNION DEFINES ITS INTERNATIONAL DIGITAL STRATEGY

dplnews - The European Union (EU) unveiled its International Digital Strategy, which has three main objectives to jointly continue the digital transformation of the member European countries. According to the EU, they will spare no effort to promote the development of new technologies, including Artificial Intelligence (AI).

LATAM CISO SUMMIT 2025: THE MOST IMPORTANT CYBERSECURITY EVENT WILL TAKE PLACE IN RIO DE JANEIRO

dplnews - Latin America is moving toward a new era of technological innovation and strengthening digital security. In this context, the Digi Americas Alliance has announced that the next edition of the LATAM CISO Summit 2025 will take place from September 11 to 13 in Rio de Janeiro, Brazil. The LATAM CISO Summit is an exclusive event that brings together the region's leading cybersecurity leaders. This year, it has the institutional support of CAF – Development Bank of Latin America, as well as the participation of the Institutional Security Office (GSI) of the Brazilian Presidency. This year, Google and CrowdStrike will be the main partners of the event.

NEW TRUMP EO AMENDS BIDEN, OBAMA ERA CYBERSECURITY RULES - USA

ExecutiveGov - President Donald Trump has issued an executive order rolling back some cybersecurity requirements from previous administrations. The White House said Friday that provisions under EO 14144, or Strengthening and Promoting Innovation in the Nation’s Cybersecurity, and 13694, or Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, have been amended.

LATIN AMERICA CYBER SECURITY MARKET TO GROW AT A CAGR OF 6.80% DURING 2025-2033

openPR - Latin America Cyber Security Market is in the midst of a sweeping transformation due to an increasing regional emphasis on digital resilience and regulations. Governments and enterprises are proactively erecting tall forts of cyber frameworks for protecting some data considered very sensitive, as the threats become higher and stricter Regulatory Standards are observed to take action.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 12, 2025

UNDERSTANDING THE EVOLVING MALWARE AND RANSOMWARE THREAT LANDSCAPE

Cybersecurity Dive - The threat landscape keeps evolving, frequently rendering traditional security measures insufficient. Effective protection mechanisms are not just beneficial; they are essential to safeguard against significant data loss, financial damage, and reputational harm that these attacks can inflict. Understanding the nature of these adversaries is the crucial first step in building robust defenses.

ZERO-TRUST, FULL STACK: EMBEDDING CYBERSECURITY PRINCIPLES INTO SITE RELIABILITY ENGINEERING CULTURE

Devops - These days, with digital threats everywhere, cybersecurity must evolve beyond just being a perimeter measure. Given the rapid delivery of software and the transient nature of infrastructure, security must be built into DevOps. This shift presents both a challenge and an opportunity for site reliability engineers (SREs) to apply zero-trust principles everywhere, starting with infrastructure and services and extending to how developers operate.