DIGI AMERICAS ALLIANCE MEMBERS

PANAMA FORMALIZES THE CREATION OF THE STATE CYBERSECURITY CENTER

La Estrella - Panama is moving toward the consolidation of its Cybersecurity Control Center, highlighted the administrator of the Government Innovation Authority, Adolfo Fábrega. On June 11, President José Raúl Mulino signed Executive Decree No. 53, which formalizes the implementation of the center for the protection of state services, information, and technological infrastructure. "We have already been awarded the first component of this center," Fábrega indicated. This is a security team that will assess the vulnerability of each state institution, and has an estimated cost of $500,000.

COSTA RICA IS PROCESSING ITS ENTRY INTO A REGIONAL CYBERSECURITY ORGANIZATION

Prensa Latina - The Ministry of Science, Technology, and Telecommunications signed the document to integrate this initiative, which offers countries in the region options for responding to cyber incidents and addresses aspects of prevention and policy effectiveness, reported the newspaper El Observador. "We celebrate this effort toward LAC4 as part of the efforts to strengthen national cybersecurity capabilities through regional and global alliances," stated Orlando Vega, the deputy minister of that ministry.

PEÑA'S GOVERNMENT OFFICIALLY LAUNCHED THE NATIONAL CYBERSECURITY STRATEGY - PARAGUAY

La Nacion - "My duty as president is for every state institution to protect citizens' data and rights with the same seriousness with which they protect their physical resources," said President Santiago Peña during the official launch of the National Cybersecurity Strategy 2025-2028. "Today we take a decisive step as a country with our National Cybersecurity Strategy, where we want to reaffirm our commitment, not only to technology, but primarily to the people. The state must be a shield; it cannot be the risk," the president said.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 20, 2025

"WE'RE FIGHTING WITH WOODEN RIFLES AGAINST LASER DRONES," SAYS EXPERT IN RESPONSE TO PARAGUAY'S EXPOSURE TO DIGITAL WARFARE

El Nacional - Paraguay is suffering a wave of cyberattacks that have exposed sensitive data belonging to public institutions. Cybercrime expert Sergio Mendoza warns that the country is defenseless, lacking laws or technology to confront this threat.

DATA CENTERS IN BRAZIL: CHALLENGES, OPPORTUNITIES AND PUBLIC POLICIES FOR A DIGITAL FUTURE

Brazil Digital Country - Data centers, or data processing centers, are physical facilities that constitute the essential pillars of contemporary digital infrastructure. They house servers, storage devices and networks, and are crucial for the massive processing and storage of digital data. In an era defined by the Information Society and the digital economy, in which digital information and the internet are central, data centers support everything from online searches and banking transactions to advanced applications in Health, Agribusiness, Industry and Cities. With the explosion in demand driven by Artificial Intelligence (AI) and increasing digitalization, the need for data center infrastructure increases exponentially.

REGISTRATION NOW OPEN FOR STF SEMINAR ON CYBERSECURITY IN THE JUDICIARY - BRAZIL

STF - Registration is now open for the 2nd International Seminar on Cybersecurity in the Superior Courts, which will be held on June 25, in the session room of the Second Chamber of the Supreme Federal Court (STF). The event is part of the STF's Information Security and Digital Integrity Week, which will take place from June 23 to 27. The seminar is aimed at representatives of the superior courts, bodies of the Brazilian and international Judiciary, Justice Councils, the private sector, academia and partner institutions.

RANSOMWARE STILL DOMINATES THE CYBERATTACK LANDSCAPE IN LATIN AMERICA: 8 OUT OF 10 INCIDENTS AFFECT THE FINANCIAL SECTOR

Clarin - “Latin America's innovative and entrepreneurial spirit doesn't come with a concern for cybersecurity.” This is one of the conclusions of a new survey on the cyber defenses of the region's financial sector, where the largest number of cases of ransomware, a type of attack that encrypts information to extort a ransom, were recorded. The paper was published this Tuesday by Duke University and Digi Americas, an organization focused on cybersecurity in the Americas. In addition to focusing on the impact of ransomware on the financial sector, it also devotes a few pages to phishing, banking Trojans, third-party attacks, and vulnerability exploitation.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 20, 2025

CYBERCRIMINALS ADOPT AGENTIC AI TO LAUNCH ATTACKS WITHOUT DIRECT HUMAN INTERVENTION

Newsinamerica - Guatemala faces a growing sophistication in the digital threat landscape, with a sustained increase in cybersecurity incident reports. According to the GT-CERT 2024 Cybersecurity Bulletin, multiple compromise events were recorded, including targeted phishing campaigns, attempts to exploit known vulnerabilities, and ransomware attacks against public and private entities. These threats highlight the need to strengthen the national cybersecurity posture, especially in critical sectors such as finance, education, and government, where digitalization is advancing rapidly.

LATIN AMERICA WILL CREATE ITS OWN ARTIFICIAL INTELLIGENCE MODEL: LATAM-GPT

Forbes - A dozen Latin American countries have joined forces to create the first large-scale artificial intelligence language that understands the region's specificities. The first version will be released in September, Chilean authorities announced Tuesday.

NIST FLAGS RISING CYBERSECURITY CHALLENGES AS IT AND OT SYSTEMS INCREASINGLY CONVERGE THROUGH IOT INTEGRATION – USA

Industrial Cyber - The U.S. National Institute of Standards and Technology (NIST) has observed in a discussion essay a growing convergence between OT (operational technology (OT) and IT, driven by the rise of the Internet of Things (IoT) and internet-connected equipment that were once isolated. OT infrastructure covers programmable systems and devices that directly interact with or control the physical environment.

THIRD-PARTY CYBER ATTACKS PUT SPOTLIGHT ON CONTINGENT BUSINESS INTERRUPTION COVERAGE

Insurance Business Magazine - A string of high-profile cyber attacks involving third-party software vendors last year has forced organizations to take a hard look at their contingent business interruption (CBI) coverage. According to one wholesale broker specializing in cyber, businesses' vulnerability to third-party outages was exemplified by two events in 2024: the Change Healthcare breach and the CDK Global attack.

HOW ENERGY AND MANUFACTURING CAN STAY AHEAD OF CYBER THREATS AND PROTECT THEIR TECH

WEF - Operational technology (OT) environments in the energy and manufacturing sectors are often outdated, poorly segmented and generally perceived as insecure. Limited internal resources and scarce cybersecurity expertise mean companies are increasingly relying on outsourcing to strengthen OT security. The rapid adoption of artificial intelligence is not only increasing energy demand but also intensifying cybersecurity risks.