DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 23, 2026

DIGI AMERICAS ALLIANCE MEMBERS

PANAMA UNVEILS ITS NEW CYBERSECURITY MONITORING CENTER

SEGURILATAM - Francisco Guinard, Deputy Administrator of the National Authority for Government Innovation (AIG), has presented Panama's new Cybersecurity Monitoring Center. This initiative aims to strengthen the State's capacity to detect, prevent, and respond to digital threats. In this way, the country will have greater visibility into risks in real time and will be able to anticipate potential incidents. "The goal is to prevent attacks or, if they occur, to contain them before they become a greater risk to citizens' data," explains the Deputy Administrator.

PANAMA DEVELOPS STRATEGY FOR EXPORTING MODERN SERVICES

Revista E&N - Panama launched Panama's National Strategy for Exports of Modern Services (ENESM-PA 2026), a roadmap that seeks to boost sectors intensive in knowledge, technology, and human talent. The initiative, led by the Ministry of Commerce and Industries (MICI), marks the transition from design to implementation after six months of technical work and coordination with the private and academic sectors.

COMMITTEE OF THE CHAMBER OF DEPUTIES APPROVES REFORMS TO PROTECT CHILDREN AND ADOLESCENTS ON THE INTERNET - MEXICO

Infobae - The Committee on the Rights of Children and Adolescents of the Chamber of Deputies has approved reforms to the General Law on the Rights of Children and Adolescents with the aim of strengthening protection against cyberbullying and digital violence, and guaranteeing the security of minors' personal data in digital environments. This legal amendment responds to the accelerated growth of risks on digital platforms and seeks to establish direct measures to prevent harmful content and protect digital identity.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 23, 2026

CYBER POLICE WARN ABOUT FAKE JOB OFFERS ON SOCIAL MEDIA - MEXICO

El Heraldo de México - Digital security specialists in Mexico have raised the alarm about the growing number of fake job offers circulating on social media and other digital platforms. These scams, which promise high salaries and benefits exceeding legal requirements, seek to exploit the financial needs of job seekers, according to cybersecurity experts. The proliferation of these deceptive ads represents a significant risk to the public. Criminals use very attractive tactics to capture the attention of those looking for employment. They offer salaries that can reach 8,000 pesos per week for roles such as promotional models, along with benefits that surpass those established by law.

MARITIME CYBERSECURITY: VALPARAÍSO PORT TERMINAL ADVANCES IN DIGITAL RISK MANAGEMENT AND PORT DATA PROTECTION - CHILE

g5noticias - Terminal Portuario Valparaíso (TPV) announced the implementation of Maritime Circular DGTM and MM O-75/006, a regulation that establishes new provisions for the management of maritime cyber risks and the protection of information in port facilities. With this milestone, TPV consolidates its position as a maritime terminal with high compliance standards, continuing the progress driven by Maritime Circular O 75/005, which establishes the implementation of a maritime cyber risk management system aligned with current regulations and international best practices.

DIGITAL INFRASTRUCTURE IS NOW CRITICAL FOR CHILE: ACTI CALLS FOR UNLOCKING INVESTMENT IN DATA CENTERS AND CLOUD

dpl news - In Chile, digital infrastructure has ceased to be merely an “IT issue” and has become a critical component of the country's operational continuity. Data centers, cloud services, connectivity, and cybersecurity now underpin payments, logistics, telecommunications, public services, healthcare, and industrial operations. When this foundation fails, essential services are disrupted, and the development of the digital economy is directly impacted.

BRAZILIAN NAVY STRENGTHENS ITS DEFENSE CAPABILITIES IN THE DIGITAL ENVIRONMENT

Defesa Net - The Brazilian Navy (MB) has expanded its operations in the cyber domain in light of the growing importance of the digital environment in contemporary conflicts. In this context, the Force activated, in August 2025, the Cyber Warfare Squadron (EsqdGCiber), an initiative that strengthens cyber defense capabilities and the protection of strategic naval systems. Contemporary wars are not limited to the use of conventional troops and weapons; they also develop in the digital environment, where systems, networks, and information become strategic targets. In this scenario, modern military strategy has begun to consider the so-called "fifth operational domain"—cyberspace or the cyber domain—which is added to the four traditional domains: land, sea, air, and space.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 23, 2026

ANTHROPIC INVESTIGATES UNAUTHORIZED ACCESS TO ITS MYTHOS AI MODEL

CR Hoy - The US artificial intelligence company Anthropic announced Tuesday that it is investigating unauthorized access to its powerful Mythos model, which the company fears could become a valuable tool for hackers. Anthropic said weeks ago that it initially limited the release of Mythos to 40 large technology firms to give them a head start in patching cybersecurity vulnerabilities before they could be exploited by attackers. According to Bloomberg, a small group of users on a private online forum gained access to the model through Anthropic's computer system reserved for external vendors.

IDB GROUP ADVANCES REGIONAL COOPERATION AT ONE CARIBBEAN MINISTERIAL DIALOGUE

IDB - The Inter-American Development Bank Group (IDB Group) launched three key regional initiatives on cybersecurity, capital market integration and fiscal policy under its regional program ONE Caribbean, that aims to foster long-term stability and growth in the Caribbean. The new actions were presented during the ONE Caribbean Ministerial Dialogue in Port of Spain, Trinidad and Tobago, a high-level gathering that marked the program’s two-year milestone. Through this leadership dialogue, IDB Governors and regional partners deliberated on emerging priorities for shaping the next phase of the program.

SEEING THE CYBER IN ECONOMIC STATECRAFT - USA

War on the Rocks - Americans lost nearly $21 billion to cybercrime in 2025, a new record for cyber-enabled economic losses. Private sector losses to malicious cyber activity regularly exceed $200 billion in a given year. Alongside criminal groups, state-sponsored hackers are increasingly targeting America’s pocketbook. Neither the economic sphere nor cyberspace are classic terrestrial warfighting domains. Yet war is being actively waged through both realms and national cyber security is vital to the prosperity and protection of today’s hyperconnected economy. China is both the greatest economic threat and the most active and persistent cyber threat to the United States. Both its economic and cyber statecraft campaigns reach deep into America’s government, private sector, and critical infrastructure. These two efforts overlap: Cyber espionage, digital theft, and supply chain compromises are key pillars of China’s strategy to undermine the U.S. economy. Addressing this challenge requires marshaling economic and cyber power into cohesive, coordinated campaigns.

UK CYBER AGENCY HANDLING FOUR MAJOR INCIDENTS A WEEK AS NATION-STATE ATTACKS SURGE

The Record - Britain's cybersecurity chief warned Tuesday that the country is handling four nationally significant cyber incidents every week, with the majority now traced back to hostile foreign governments rather than criminal hackers, as the government unveiled a £90 million (about $121.48 million) package to bolster the country's digital defences. Richard Horne, chief executive of the National Cyber Security Centre (NCSC), told the annual CYBERUK conference in Glasgow that while the incident rate had held relatively steady since he first disclosed the figure last October, the origin of those attacks had shifted dramatically.