DIGI AMERICAS LATAM CISO

INSIGHTS

NOVEMBER 20, 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

BRAZILIAN ARMY REINFORCES DIGITAL SECURITY AT COP30

Last Second - The Armed Forces have set up a special cyber defense scheme to protect information technology infrastructures during COP30 in Belém. The action is part of Operation Marajoara and focuses on preventing intrusions, digital attacks, and any attempt to compromise essential services. The Joint Cyber Warfare Detachment, subordinate to the Cyber Defense Command (ComDCiber), operates from the Integrated General Headquarters (QGI). From a Command and Control Vehicle, military personnel continuously monitor the entire IT network used by the Marajoara Joint Command.

ACCORDING TO THE INTERNET STEERING COMMITTEE, ANPD IS THE COORDINATOR OF ARTIFICIAL INTELLIGENCE REGULATION - BRAZIL

Digital Convergence - The Brazilian Internet Steering Committee defends the need for regulation "focused on protecting people" and aligned with Brazil's socioeconomic and scientific development in a public statement regarding the legal framework for artificial intelligence, as part of the progress of bill 2.338/23 in the Chamber of Deputies. The committee affirms its support for the creation of specific rules for AI systems and emphasizes that bill 2.338/2023 represents an appropriate starting point for legislative debate.

INSS (BRAZILIAN NATIONAL SOCIAL SECURITY INSTITUTE) BEGINS USING ELECTRONIC POWER OF ATTORNEY TO STRENGTHEN DATA PROTECTION AND DIGITAL SECURITY - BRAZIL

Cryptoid - Meu INSS now offers a new electronic power of attorney functionality, developed by the Ministry of Management and Innovation in Public Services (MGI) in partnership with the National Institute of Social Security (INSS). The initiative, announced on Thursday (13), strengthens cybersecurity, improves the protection of personal data and expands access to digital services. With the tool, the user can authorize a representative to access INSS services without having to share their GOV.BR password and without having to go to an agency.

DIGI AMERICAS LATAM CISO

INSIGHTS

NOVEMBER 20, 2025

MEXICO LAUNCHES THE LARGEST PUBLIC AI AND CODING SCHOOL IN THE AMERICAS, THE FEDERAL GOVERNMENT ANNOUNCES

Wired – The Mexican federal government unveiled the Public Training Center for Artificial Intelligence (AI), a project under the “Mexico: Country of Innovation” initiative, which aims to train 25,000 people annually in areas related to emerging technologies. The announcement was made at the facilities of the National Technological Institute of Mexico (TecNM) in the Tláhuac borough and was led by Claudia Sheinbaum, President of Mexico, who noted that the new educational institution will be linked to the SaberesMx platform, a digital tool offering courses and materials from various universities with the goal of “democratizing access to knowledge.”

2026 WORLD CUP: CYBERSECURITY STRENGTHENED TO CURB TICKET SCALPING AND PROTECT FANS - MEXICO

LJA.MX - The countdown to the 2026 World Cup is on, and along with the excitement for the matches to be held in Mexico, concerns are also growing about the security of ticket purchases and resales. To prevent fraud, abuse, and digital risks, the Federal Consumer Protection Agency (Profeco) announced a package of measures that includes monitoring, direct assistance, and cybersecurity actions to protect fans.

During the morning press conference on November 18, the Mexican government presented the "Social World Cup" strategy, where Profeco confirmed that it will work in coordination with FIFA to guarantee transparent processes and secure transactions both physically and digitally.

CYBERSECURITY WITH SOCIAL IMPACT: EDUCATIONAL MODEL TRANSFORMS OPPORTUNITIES IN DESAMPARADOS - COSTA RICA

El Mundo - An innovative educational project is demonstrating how technology can be a driver of opportunity for young people. At the La Libertad Foundation, a cultural space focused on community development, an unprecedented cybersecurity training model has been established in Latin America. Created in partnership with the technology industry and academia, it is aimed at young people in Desamparados.

EUROPEAN UNION LAUNCHES DIGITAL PACKAGE; PROMISES SIMPLER RULES TO ENCOURAGE INNOVATION

DPL News – “European companies will spend less time on administrative work and compliance and more time on innovation,” the European Union promised after launching a package of measures aimed at streamlining regulations on Artificial Intelligence (AI), cybersecurity, and data, with the goal of achieving estimated savings of €5 billion by 2029. Furthermore, “European business portfolios could unlock an additional €150 billion in savings for companies each year,” it calculated. The proposed changes fall under three pillars: 1. Digital Omnibus, 2. Data Union Strategy, and 3. European Business Portfolio.

TRUMP'S CYBER STRATEGY WILL EMPHASIZE ADVERSARY DETERRENCE, INDUSTRY PARTNERSHIPS - USA

Cybersecurity Dive - The Trump administration's top cybersecurity official on Tuesday previewed the contours of the administration's cyber strategy, saying it would focus heavily on countering foreign adversaries and reducing regulatory burdens on industry. “We are striving as an administration to make sure that there is a single coordinated strategy in this domain in a way that hasn't happened before,” National Cyber Director Sean Cairncross said at the Aspen Cyber Summit. “We are working in very close partnership with our interagency colleagues to develop this strategy and get it out the door.”

CISA UNVEILS GUIDE TO COMBAT BULLETPROOF HOSTING CYBERCRIME - USA

CISA - Today, the Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with US and international partners, released Bulletproof Defense: Mitigating Risks from Bulletproof Hosting Providers. This guide offers internet service providers (ISPs) and network defenders an in-depth overview of this cybercriminal activity along with key steps, best practices and resources to safeguard their customers and their networks. Developed through the Joint Ransomware Task Force, a U.S. interagency body, this guide ensures a unified approach to combat the escalating threat of ransomware attacks. Cybercriminal actors are increasingly leveraging Bulletproof Hosting (BPH) infrastructure to conduct cyber operations targeting critical infrastructure, financial institutions, and other high-value targets. BPH providers market their infrastructure as “bulletproof” to cybercriminals because they neither engage in good faith with legal processes nor with third-party or victim complaints of malicious activity enabled from such infrastructure.

US, UK AND AUSTRALIA SANCTION RUSSIAN CYBER FIRMS OVER RANSOMWARE LINKS

Reuters - The United States, Australia and Britain announced coordinated sanctions on Wednesday against Russia-based web company Media Land, accusing it of supporting ransomware operations. U.S. Treasury's Office of Foreign Assets Control also designated three members of the Russian company's leadership and three of its sister companies, the Department of Treasury said in a statement. "These so-called bulletproof hosting service providers like Media Land provide cybercriminals essential services to aid them in attacking businesses in the United States and in allied countries," said John Hurley, under secretary of the treasury for terrorism and financial intelligence.

CYBERSECURITY COALITION PUSHES REGULATORY ALIGNMENT, LEGISLATIVE ACTIONS AFTER GOVERNMENT SHUTDOWN - USA

Inside Cyber - The Cybersecurity Coalition is laying out a plan for the Trump administration and lawmakers to address pressing issues following the government shutdown, including clarification of cyber leadership roles and regulatory realignment on incident reporting. “As federal operations resume, it is imperative that the federal government renew its commitment to cybersecurity and operational resilience, dedicating the necessary attention and resources to protect Americans and safeguard U.S. economic and national security against these growing threats,” according to a Nov. 18 letter from the Cybersecurity Coalition. The letter says, “To that end, the Cybersecurity Coalition outlines four key areas of action for the Trump Administration and Congress to strengthen the nation's cybersecurity posture in the coming months.”