DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 1, 2026

DIGI AMERICAS ALLIANCE MEMBERS

WAVE OF CYBERATTACKS REVEALS NEED TO PROTECT CRITICAL INFRASTRUCTURE IN GUATEMALA

Prensa Libre – Like a domino effect, the databases of at least ten state institutions were attacked by a group of cybercriminals throughout April and May. The sequence began with the General Directorate of Arms and Ammunition Control (Digecam) of the Ministry of Defense. Four days later, the attack reached the National Health Laboratory of the Ministry of Public Health. Then, the extraction of records from more than 200,000 people from the Ministry of Labor's "Tu Empleo" (Your Job) portal was reported.

NATIONAL PUBLIC CYBERSECURITY AGENCY FIRST RATING OF VITAL OPERATORS - CHILE

Carey – The National Cybersecurity Agency (ANCI) published the results of the public consultation for the second stage of the first qualification process for Operators of Vital Importance (OIV), in accordance with Law No. 21,663, the Cybersecurity Framework Law, and its Qualification Procedure Regulations (Supreme Decree No. 285 of 2024). The next milestone is the publication of the final list of OIVs, which is expected in approximately 30 days.

AI AND CYBERSECURITY LEADERS, ALONG WITH CISOS, WILL DISCUSS THE CHALLENGES OF THE DIGITAL ECONOMY IN MEXICO

EFE - Global leaders in artificial intelligence (AI), cybersecurity, and digital resilience will meet from September 10-12, 2026, in Cancún, Mexico, to discuss the main challenges facing the digital economy in Latin America at the fifth edition of the Digi Americas LATAM CISO Summit. This year's summit will feature more than 400 senior executives, government officials, CISOs, and technology leaders from over 20 countries, including former President Iván Duque of Colombia and Toomas Hendrik Ilves of Estonia. According to Belisario Contreras, Executive Director of the Digi Americas Alliance, the goal of the event is to bring together "the people who will truly shape the region's digital future," fostering high-level dialogue among government and business leaders and experts to strengthen digital resilience and accelerate a secure digital transformation in the Americas.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 1, 2026

NATIONAL CYBERSECURITY PLAN: CHALLENGES AND QUESTIONS THAT GO BEYOND A SIX-YEAR TERM - MEXICO

Abogacia – Cybersecurity can no longer be understood as a purely technical matter. It is now an integral part of national security, personal data protection, institutional continuity, the provision of digital public services, and public trust in the State. In Mexico, its importance has grown due to the intensive use of digital technologies, the increase in cybercrime, the expansion of banking, online services, the digitization of government procedures, e-commerce, and the rapid advancement of artificial intelligence-based tools.

CNCIBER PRESENTS A GOVERNANCE MODEL FOR NATIONAL CYBERSECURITY - BRAZIL

Convergencia Digital - During the public hearing that discussed Bill 4.752/2025, which creates the Legal Framework for Cybersecurity in Brazil and the National Program for Digital Security and Resilience, Marcelo Malagutti, executive secretary of the National Cybersecurity Committee (CNCiber), presented a governance model for cybersecurity in Brazil, organized from the various bodies that already work on the subject. The debate took place in the Senate's Science and Technology Committee, this Tuesday, 30.

BRAZIL COULD BE LATIN AMERICA'S COMPASS FOR ONLINE CHILD SAFETY

DPL News - Even though it's not specifically designed for them, technology is already part of the daily lives of children and teenagers around the world. That's why the debate about online safety for children is gaining increasing importance on the international stage. When a teenager opens a social network on their phone, the space for learning, entertainment, and connecting with friends can also be a gateway to risks such as harassment, exposure to harmful content, or contact with strangers.

WORLD BANK ADVOCATES FOR CYBERSECURITY AND PRODUCTIVE USE OF CONNECTIVITY IN BRAZIL

Tele.Sintese - The World Bank argued that Brazil should prioritize cybersecurity and the productive use of connectivity in the next stage of its digital agenda. This assessment was made by Luciano Charlita de Freitas, senior specialist in Digital Development and Artificial Intelligence at the institution, during a panel at the Digital Nation Summit, held by GSMA in Brazil, this Tuesday, the 30th, in São Paulo.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 1, 2026

GOVERNMENT LAUNCHES RANSOMWARE PREVENTION AND RESPONSE GUIDE TO GUIDE MANAGERS AND PUBLIC SERVANTS - BRAZIL

gov.br - To guide managers and public servants, the Ministry of Management and Innovation in Public Services (MGI), in partnership with the Center for Research and Development in Telecommunications (CPQD), released, this Wednesday (July 1st), the Guide to Prevention and Response to Ransomware. Developed within the scope of the Inspire Project, the publication aims to serve as a reference on the main measures for preventing and responding to ransomware attacks, which use encryption techniques to hijack data and block computer assets, usually conditioning the restoration of access on the payment of a ransom. The initiative is part of the Privacy and Information Security Program (PPSI), conducted by the Digital Government Secretariat (SGD) of the MGI.

US LIFTS EXPORT CONTROLS ON ANTHROPIC'S FABLE 5 AND MYTHOS 5 MODELS

Noticias Neo - US lifts export controls on Anthropic's Fable 5 and Mythos 5 models. The US company Anthropic has announced that the US Department of Commerce has decided to lift the export controls affecting its artificial intelligence models, Claude Fable 5 and Mythos 5. This decision will allow the company to restore access to these models starting tomorrow.

CHECK POINT (CHKP) INTEGRATES CUTTING-EDGE OPENAI MODELS INTO ITS SECURITY SUITE

Noticias Neo - Check Point integrates cutting-edge OpenAI models into its security suite. Check Point Software Technologies Ltd. has taken a significant step in the field of cybersecurity by announcing the integration of OpenAI's advanced artificial intelligence capabilities into its security products. This collaboration, formalized through the OpenAI Daybreak Cyber Partner Program, represents an evolution in the company's strategy, moving from using internal models to directly incorporating next-generation artificial intelligence into the tools and workflows that businesses use daily.

INSIDE THE INFRASTRUCTURE OF MODERN SEO POISONING: BULLETPROOF HOSTING AND INDUSTRIAL-SCALE EVASION

Lumu Technologies - Cybercriminals are changing their tactics. They no longer rely on email to steal credentials or intercept funds. Instead, threat actors use SEO poisoning to place fake payment portals at the top of search engine results. SEO poisoning is a strategy that tricks users into clicking malicious links during routine transactions. Fraudsters place fake pages at the top of search engine results to deceive users. Users see these links in google and click on them with high confidence.