DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 15, 2026

DIGI AMERICAS ALLIANCE MEMBERS

PANAMA STRENGTHENS DIGITAL SECURITY AFTER A WAVE OF CYBERATTACKS AGAINST THE STATE

EnSegundos.com.pa - The government launched a prevention, detection, and response plan on Monday to strengthen state cybersecurity through advanced technology following a wave of cyberattacks on the public sector amidst a bureaucratic digitization process, reported the EFE news agency. “For the past few years, the focus has been on progressively raising the level of digital maturity of institutions. But the global context has evolved rapidly, and the level of threat requires moving toward much more robust standards,” said Adolfo Fábrega, general administrator of the National Authority for Government Innovation (AIG).

COMPANIES IN MEXICO AND CENTRAL AMERICA ARE ACCELERATING RISK MANAGEMENT IN THE FACE OF PRESSURE FROM AI, CYBERSECURITY, AND TALENT

dpl news – Artificial Intelligence (AI), cybersecurity, and talent shortages are the main challenges for companies in Mexico and Central America in 2026, reveals the study "Risks in Mexico and Central America 2026." In Mexico, 81% of companies consider changes in the geopolitical environment to be the main short-term risk, followed by cyberattacks at 79%. Furthermore, 65% identify the failure to leverage the advantages of using AI as a threat, and the same percentage warn of difficulties in attracting or retaining talent.

CYBERCRIME INTENSIFIES DISPUTE FOR DIGITAL TALENT AMID SHORTAGE OF SPECIALISTS IN MEXICO

Coworking - Digitally skilled talent in Mexico has become attractive to cybercrime networks, intensifying competition between companies and criminal groups to recruit specialists in areas such as software development, vulnerability analysis, and technological infrastructure.

DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 15, 2026

COLOMBIA | TEXT MESSAGE SCAMS CONTINUE TO GROW AND NOW USE ARTIFICIAL INTELLIGENCE

dpl news - Digital scams via text message continue to grow in Colombia and are reaching new levels of sophistication thanks to the use of artificial intelligence. Technology sector experts warned that smishing, a type of SMS-based fraud, has become a common method used by criminals to steal financial and personal information through messages that appear to come from official entities or well-known companies.

DGA IMPLEMENTS ICT TO STREAMLINE INSTITUTIONAL TECHNOLOGY SERVICES - DOMINICAN REPUBLIC

Presidency.gob.do - Santo Domingo - The General Directorate of Customs (DGA) has launched the ICT (Information and Communication Technologies) Observability Center, a key initiative aimed at strengthening the supervision, stability, and continuity of institutional technology services. This center will allow DGA teams to constantly monitor the technological infrastructure, critical applications, networks, security, and digital services that support the country's customs operations.

NICARAGUAN ARMY PARTICIPATES IN REGIONAL COURSE ON CYBER THREATS

Nueva Ya - In compliance with the orders of the Commander-in-Chief of the Nicaraguan Army, General Julio César Avilés Castillo, the institution participated on May 11, 2026, in the opening of the Cyber Threats Course. This training is being provided by the Communications Brigade of the Guatemalan Army, as part of the schedule of activities for the Conference of Central American Armed Forces (CFAC).
The course, which runs from May 11 to 15, has the participation of 50 specialist officers from Guatemala, El Salvador, Honduras, Nicaragua and the Dominican Republic.

COSTA RICA DECLARES CYBERSECURITY TALENT DEVELOPMENT TO BE IN THE PUBLIC INTEREST

CR Hoy - Cybersec Cluster announced that the development of local cybersecurity talent has been declared a matter of public interest. The declaration, made by the Ministry of Science, Innovation, Technology and Telecommunications (MICITT), encompasses two initiatives: the formation, training, and participation of the national cybersecurity team in regional and international competitions, as well as the Cybersec Challenge 2026, in all its editions and formats. According to Carolina Taborda, general manager of the Cybersec Cluster, the development of the cybersecurity team and the strengthening of the Cybersec Challenge reflect Costa Rica's commitment to building specialized talent.

DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 15, 2026

IFC AND BAC PROMOTE CREDIT FOR MSMES

Republica – The International Finance Corporation (IFC), the World Bank Group's private sector arm, announced a $230 million investment in BAC Guatemala to expand credit to micro, small, and medium-sized enterprises (MSMEs). The operation aims to strengthen sustainable finance and boost job creation in the country. IFC will grant BAC Guatemala a $200 million long-term loan and a $30 million trade finance facility. These resources will allow the bank to expand its financing portfolio for MSMEs, a sector that has historically faced difficulties accessing credit in Guatemala.

ANTHROPIC'S MYTHOS FORCES BANKS TO FIX THEIR CYBER VULNERABILITIES

Forbes Mexico – US banks are scrambling to correct numerous weaknesses in their computer systems detected by Anthropic’s powerful but expensive AI tool, Mythos, prompting urgent repairs, software updates, and the potential for service disruptions for customers. Some of the nation’s largest banks have access to Mythos and are now uncovering the problems the program reveals, according to several sources familiar with the matter.

CYBERSECURITY COMPANIES WARN OF RISKS FROM AI IMPLEMENTATION IN ORGANIZATIONS

Forbes Central America – Batuta, Cloudflare, and Sophos, cybersecurity companies, warned of a trend documented in various analyses: organizations are accelerating the implementation of artificial intelligence (AI) while underestimating existing security risks. Digi Americas released a statement detailing the results and conclusions of several studies conducted by these companies on the risks that AI poses to organizational security.

SOFTWARE BILL OF MATERIALS FOR AI - MINIMUM ELEMENTS - USA

CISA - CISA and the Group of Seven (G7) international partners—Germany, Canada, France, Italy, Japan, the United Kingdom, and the European Union—have released joint guidance, Software Bill of Materials for AI – Minimum Elements, to help public and private sector stakeholders improve transparency in their artificial intelligence (AI) systems and supply chains. A software bill of materials (SBOM) acts as an “ingredients list” for software that better positions organizations to understand their supply chains and make risk-informed decisions about how to protect their critical systems. The guidance builds on CISA’s previous work with federal and international partners to establish a shared vision for a software bill of materials and provides recommendations on minimum elements that should be included in an SBOM for AI. Because AI systems are software systems, these recommendations should be considered in addition to the general minimum elements for an SBOM.