DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 12, 2026

DIGI AMERICAS ALLIANCE MEMBERS

THE DOMINICAN REPUBLIC WILL ESTABLISH ITS NEW CYBER CLUSTER TO STRENGTHEN NATIONAL CYBERSECURITY

The Dominican Republic will take another step in strengthening its digital security ecosystem with the official establishment of the Dominican Republic Cyber Cluster, a collaborative initiative that will bring together leading companies, strategic organizations, and key players in the technology and cybersecurity sectors. The official signing ceremony will take place in the auditorium of the INDOTEL Digital Culture Center, in an exclusive gathering for 50 special guests from the business, technology, and institutional ecosystem.

EL SALVADOR PROMOTES CYBERSECURITY AS AN ENGINE FOR DEVELOPMENT AND COMPETITIVENESS

Digital Shield - With the aim of helping companies protect their data, avoid attacks of computer, digital, electronic, virtual and computational origin, and understand the risks associated with the use of artificial intelligence in fraud, the Chamber of Commerce and Industry of El Salvador (Camarasal), through its Technology Committee, recently convened the so-called CyberWeek 2026, focused on business cybersecurity.

PANAMA, A LOGISTICS HUB FACING GROWING CYBER RISKS

Summa Magazine - Panama has established itself as one of Latin America's leading logistics and financial hubs. Its interoceanic canal, ports, airports, submarine cables, and financial system connect it to the global economy, but this very importance has made it an increasingly attractive target for cybercrime. Between 2025 and 2026, cyberattacks increased by 25%, reaching an average of 2,600 malicious attempts per week per organization and more than 3,300 in the financial sector. In May 2026 alone, 1.17 terabytes of data were compromised, while recent incidents in banking and healthcare have placed the country among those most affected by data breaches on the dark web.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 12, 2026

CYBERSECURITY EXPERT EXPLAINS IMPORTANCE TO THE ECONOMY COMMITTEE DRAFTING NEW BILL - GUATEMALA

LaHora.gt - The Legislative Committee on Economy and Foreign Trade is discussing the Cybersecurity Law after the Plenary decided to return Bill 6347 to the committee for a new report, as several deputies and sectors opposed the proposal that had advanced in the Chamber. Previously, only the Committee on National Security Affairs had issued a report on the bill, but now both committees will present separate reports to begin its approval process in the Chamber.

BERMUDA WELCOMES GOOGLE SUBSEA CABLE LANDING

Marine Technology News - The Government of Bermuda welcomed the landing of Google's Nuvem and Sol subsea cable systems in Bermuda, describing the milestone as an investment in the island's digital infrastructure, economic resilience, and long-term competitiveness. The Nuvem and Sol cable systems will strengthen international connectivity, enhance network resilience, and support the growing demand for secure, reliable digital infrastructure worldwide.

CLAUDE FABLE 5 MARKS A NEW ERA OF AI WITH PROGRAMMED SAFETY LIMITS; UNDERSTAND WHY

Times Brasil - Anthropic has unveiled Claude Fable 5, a new artificial intelligence model that marks a significant shift in how the company delivers advanced systems. The offering combines enhanced performance capabilities with an integrated security mechanism that automatically limits access to content deemed dangerous. The model belongs to the so-called "Mythos class," a generation of AI that, until now, had its use limited to testing due to the high risk of misuse. Now, with Fable 5, Anthropic expands access but maintains strict control over sensitive topics. In practice, the system operates in a hybrid manner. Claude Fable 5 normally responds to user requests, but when it identifies questions related to topics such as offensive cybersecurity or potentially dangerous biological research, it does not respond directly.

WHAT MAJOR CHALLENGES DOES LATIN AMERICA AND THE CARIBBEAN FACE IN STRENGTHENING ITS CYBERSECURITY?

SeguriLATAM - Cybersecurity remains one of the challenges facing Latin America and the Caribbean. This is the conclusion of the Cybersecurity Report 2025: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean, prepared by the Organization of American States. The report warns that the region still faces significant gaps in maturity, capabilities, and resources in the face of an increasingly complex digital environment exposed to threats. One of the main challenges identified is inequality in cybersecurity. The report indicates that countries in the region have some of the lowest levels of self-assessed cyber resilience globally, a situation that makes them more vulnerable to attacks capable of affecting critical infrastructure, essential services, economic activity, and public trust in digital systems.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 12, 2026

CISA ISSUES BINDING OPERATIONAL DIRECTIVE OUTLINING STEPS FOR AGENCIES TO ADDRESS VULNERABILITY MANAGEMENT - USA

Inside Cybersecurity - The Cybersecurity and Infrastructure Security Agency has issued a binding operational directive ordering civilian agencies to take steps on vulnerability management through a risk-based approach based on four criteria areas, as part of the government's work to implement a June 2 executive order on frontier artificial intelligence models. "In 2021 CISA established the Known Exploited Vulnerabilities catalog pursuant to BOD 22-01, which directed agencies to aggressively remediate known exploited vulnerabilities (KEVs), protect federal assets, and reduce cyber incidents.

WARNER PROPOSES BILL TO FORCE CISA UPDATES TO CRITICAL INFRASTRUCTURE CYBERSECURITY PLANS AMID AI-DRIVEN THREATS - USA

Industrial Cyber - A U.S. Senator introduced a bill that would require the Cybersecurity and Infrastructure Security Agency (CISA) to update cybersecurity plans across all critical infrastructure sectors and assess emerging technology-driven risks. Titled 'Combat Emerging Threats to Critical Infrastructure Act of 2026,' the legislation comes amid growing concerns that advances in AI (artificial intelligence) could accelerate cyberattacks against essential services and critical infrastructure. Warner said the measure is intended to ensure that government, industry, regulators, and cybersecurity experts regularly refresh defensive plans to address increasingly sophisticated threats, including those enabled by AI.

THE CYBER THREAT TO THE 2026 WORLD CUP

CSIS - Major events present a vastly expanded attack surface—but also tend to act as a mirror, reflecting the geopolitical tensions of the moment. The 2026 FIFA World Cup takes the usual complexity of a major event and multiplies it on three fronts: First, it takes place across three international jurisdictions (the United States, Canada, and Mexico), and 16 host cities within them. Second, it significantly scales the digital attack surface across networks, supporting digital infrastructure and the millions of mobile devices present. And third, it takes place against the backdrop of ongoing geopolitical conflicts, including the Russia-Ukraine war and the now reignited U.S.-Israel-Iran conflict—but also coincides with the United States' 250th anniversary celebrations. Alone, each front presents its own type of cyber risk, but together, they present a cumulative set of risks that makes securing this tournament somewhat unique.

CHECK POINT REPORTS RANSOMWARE ATTACKS JUMP 48% YEAR OVER YEAR DESPITE DECLINE IN OVERALL CYBERATTACK ACTIVITY

Industrial Cyber - Global cyberattack activity eased in May 2026 following April's sharp rebound, but the broader threat landscape remained volatile, according to research from Check Point Research. Organizations experienced an average of 2,055 weekly cyberattacks during the month, representing a 2% increase year-over-year despite a 7% decline from April. Education remained the most targeted sector, averaging 4,641 weekly attacks per organization, while government and telecommunications also continued to face elevated attack volumes.