DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2026

DIGI AMERICAS ALLIANCE MEMBERS

FINANCIAL INSTITUTIONS MUST ADAPT TO NEW CYBERSECURITY REQUIREMENTS - BRAZIL

Infor Channel - Financial institutions authorized to operate by the Central Bank of Brazil have until March 1st to comply with the new Cybersecurity requirements established by CMN Resolution No. 5,274/2025, published last December by the National Monetary Council. This Resolution amends CMN Resolution No. 4,893/2021, which deals with the Cybersecurity policy and the requirements for contracting data processing and storage services and cloud computing to be observed by financial institutions.

QUANTUM COMPUTING IN 2026: HOW THE NEW TECHNOLOGY COULD REDEFINE GLOBAL SECURITY - BRAZIL

RealTime1 - While artificial intelligence dominates the public debate, an even more profound transformation is advancing in the laboratories of major powers: quantum computing. Unlike traditional computers, which operate with bits (0 and 1), quantum machines use qubits, capable of processing multiple states simultaneously. The potential is disruptive. Quantum computing promises to solve problems considered intractable by current supercomputers — from the discovery of new materials to complex logistical optimization. But there is a critical point: digital security.

2026 WORLD CUP PUTS CYBERSECURITY TO THE TEST - MEXICO

Yo Influyo - Mexico is preparing to host one of the most important sporting events on the planet: the 2026 FIFA World Cup. Expectations are focused on logistics, the economic impact, and tourism, but there is another front already generating concerns among authorities and specialists: digital security. The combination of millions of visitors, a rapid increase in e-commerce, and the massive handling of personal data is placing the country's technological infrastructure under unprecedented pressure. The tournament, which Mexico will share with the United States and Canada, will entail an extraordinary increase in electronic transactions, online services, digital purchases, and real-time financial operations.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2026

IDENTITY EMERGES AS CYBERSECURITY'S NEW CONTROL LAYER - MÉXICO

Mexico Business News - Cyber risk keeps escalating from a technical issue to a systemic economic and reputational threat. Mexico's rise among the most targeted ransomware markets, combined with projections of tens of millions of additional attacks tied to the 2026 World Cup, reinforces that scale events now amplify national attack surfaces. The landmark acquisition of CyberArk by Palo Alto Networks formalized identity security as foundational to zero trust and AI-era defense. Simultaneously, LLM-enabled malware demonstrated that advanced attacks no longer require advanced skills. The narrative is clear: cybersecurity investment is moving from reactive defense to ROI-driven identity governance as a board-level priority.

TREASURY ANNOUNCES PUBLIC-PRIVATE INITIATIVE TO STRENGTHEN CYBERSECURITY AND RISK MANAGEMENT FOR AI - USA

U.S. Treasury - In support of the President's AI Action Plan, the U.S. Department of the Treasury today announced the conclusion of a major public-private initiative to strengthen cybersecurity and risk management for artificial intelligence (AI) in the financial services sector. Over the course of February, Treasury will release a series of six resources developed in partnership with industry and federal and state regulatory partners to enable secure and resilient AI across the U.S. financial system. "As this Administration has made clear, it is imperative that the United States take the lead on developing innovative uses for artificial intelligence, and nowhere is that more important than in the financial sector," said Secretary of the Treasury Scott Bessent. "This work demonstrates that government and industry can come together to support secure AI adoption that increases the resilience of our financial system."

DOD LEADERS WARN AI, CRYPTOCURRENCY 'LOWERS THE BAR' FOR CYBERCRIMINALS - USA

Defense Scoop - Top Defense Department officials focused on combating cybercrime said Thursday that artificial intelligence and cryptocurrency are making it easier for nefarious actors to threaten national security and circumvent traditional financial tracking systems. The warning comes amid what the officials described as a rapidly changing threat environment, one that allows for low-level criminals to adopt sophisticated cyber exploitation methods and adversarial countries to obscure their actions, often in tandem.

ECLAC WARNS THAT DIGITAL FRAGILITY THREATENS STABILITY IN THE CARIBBEAN

The Economic Commission for Latin America and the Caribbean (ECLAC) warned that the structural vulnerability of the Caribbean's digital infrastructure could compromise the economic stability and governmental continuity of its member states, and proposed creating an international backup mechanism to protect critical information from natural disasters, cyberattacks, and connectivity failures. This is according to the study "Data Embassies: An Innovative Approach to Strengthening Digital Resilience in the Caribbean," authored by Tyra Greene and Dimitris Heráclеo, and presented virtually by the regional body.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2026

DIGITAL CRIME IS NOW OPERATING AT RECORD SPEED, AND IDENTITY IS BECOMING THE NEW VULNERABILITY

Technocio - In 2025, the fastest 25% of attacks stole data in 72 minutes, and 87% of intrusions crossed multiple surfaces simultaneously. Unit 42, the incident response and investigation team at Palo Alto Networks, published its Global Incident Response Report 2026, an analysis of more than 750 cases handled between 2024 and 2025. The report reveals a shift in the pace of cybercrime and confirms that identity—that is, user accounts and permissions that grant access to systems and data; for example, an employee's username and password—is now the most common way to gain entry and access within organizations. In 2025, the fastest 25% of attacks stole data in 72 minutes, and 87% of intrusions crossed multiple surfaces simultaneously. Furthermore, nearly 90% of the investigations included identity failures as a determining factor, and 99% of cloud identities had excessive privileges.

CYBERSECURITY AND RESILIENCE IN ESSENTIAL SERVICES

Segurilatam - In a global landscape marked by uncertainty, interdependence, and the rise of hybrid threats, protecting essential services and the critical infrastructure that supports them has become a strategic priority for every country. However, this is not a recent concern. In Spain, attention to these assets dates back at least to 2011, with the development of Law 8/2011, which established measures for the protection of critical infrastructure and already recognized the growing dependence of these services on information and communication technologies.

NEW ALLIANCE BETWEEN CLOUDFLARE AND MASTERCARD AUTOMATES DEFENSE AGAINST CYBER THREATS

Panama24Horas - Cloudflare, a cloud connectivity company, and Mastercard announced a strategic partnership designed to develop protection tools for small businesses, critical infrastructure, and governments. The main objective of this agreement is to defend these organizations against current cyber threats without hindering their capacity for technological innovation. The alliance combines Mastercard's Recorded Future and RiskRecon attack surface monitoring capabilities with Cloudflare's suite of application security solutions. This partnership allows millions of users to map, prioritize, and automate the remediation of hidden risks in their internet-connected environments through a unified platform.

EVOLVING RANSOMWARE TACTICS WITH AI-ENHANCED ATTACKS AND RANSOMWARE AS A SERVICE

FinancierWorldwide - The UK government has estimated that the cost of cyber attacks to UK businesses is more than £14bn and suggests that the UK is the most targeted country by threat actors in Europe. According to a 2025 survey by the Home Office, 612,000 businesses identified a cyber attack in the preceding 12 months – and those are just the businesses that submitted a report, with the true figure likely to be significantly higher. Developments in ransomware as a service (RaaS) and subsequently artificial intelligence (AI) have led to these attacks becoming increasingly sophisticated and complex, meaning more than ever businesses need to proactively manage and improve the resilience of their systems.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2026

CYBERSECURITY GUIDANCE FOR DATA CENTER POWER AND COOLING INFRASTRUCTURE SYSTEMS

Data Center Dynamics - Network connected power, cooling, and environmental systems increase operational visibility and efficiency but also expand the cyber attack surface. This whitepaper outlines a practical framework to evaluate vendors, harden OT networks, and embed cybersecurity across design, installation, and operations. Vendor security maturity and lifecycle alignment: How to assess secure development lifecycle practices, independent certifications, vulnerability management processes, and transparency to ensure infrastructure is secure by design. Defense in depth and zero trust network architecture: Best practices for perimeter hardening, VLAN segmentation, firewall configuration, encrypted protocols, least privilege access, and continuous verification across OT environments. Operational vigilance and incident readiness: How to maintain firmware updates, preserve security settings, monitor anomalies, implement structured incident response plans, and leverage managed cybersecurity services to sustain resilience over time.

THE CYBER THREATS TO WATCH IN 2026 – AND OTHER CYBERSECURITY NEWS

WEF - Accelerating AI adoption, geopolitical fragmentation and widening cyber inequity are reshaping the global risk landscape, finds the latest Global Cybersecurity Outlook from the World Economic Forum.
Based on data from 800 global leaders, the 2026 report reveals that as attacks grow faster, become more complex and unevenly distributed, organizations and governments face rising pressure to adapt amid persistent sovereignty challenges and widening capability gaps. In the face of these challenges, three clear themes emerge: AI is supercharging the cyber arms race, geopolitics is a defining feature of cybersecurity, and cyber-enabled fraud is threatening CEOs and households alike.

HACKERS EXPLOIT ZERO-DAY FLAW IN DELL RECOVERPOINT FOR VIRTUAL MACHINES

Cybersecurity Dive - Threat actors are weaponizing a zero-day vulnerability in Dell RecoverPoint for Virtual Machines in a cyberattack campaign that drops a novel backdoor, according to new findings from Mandiant and Google Threat Intelligence Group. The product allows users to manage backup and disaster recovery for VMware virtual machines. The vulnerability, listed as CVE-2026-22769, is a hardcoded credential vulnerability that can allow an unauthenticated attacker to gain access to an underlying system and maintain root-level persistence. The vulnerability has a severity score of 10.