DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 2, 2026

DIGI AMERICAS ALLIANCE MEMBERS

NATIONAL ASSEMBLY APPROVES ORGANIC LAW FOR THE STRENGTHENING OF CYBERSECURITY - ECUADOR

Ecuador Communication - With 83 votes in favor, the Plenary of the National Assembly resolved the partial objection to the Organic Law Bill for Strengthening Cybersecurity, based on the non-binding report of the Commission on Sovereignty, Integration, and Comprehensive Security. The law establishes a modern and constitutionally compatible framework to strengthen national cybersecurity, protect critical infrastructure, and guarantee the continuity of essential services. Furthermore, it articulates a coherent model of digital governance.

COLOMBIA 5.0: THE COMMITMENT TO A DIGITAL TRANSFORMATION WITH A TERRITORIAL FACE

elcampesino.co - Colombia is embarking on a new stage in its journey toward digital transformation. With the launch of Colombia 5.0, the Ministry of Information and Communications Technologies presents a vision that puts technology at the service of territorial development, equity, and competitiveness, moving beyond a focus solely on technological adoption. This initiative marks the evolution from Colombia 4.0 to a model aligned with the concept of Society 5.0, in which innovation is directly linked to the needs of individuals, communities, and productive sectors.

CYBERATTACKS AND TECHNICAL FAILURES INCREASE THE RISK OF DATA LOSS: EXPERTS CALL FOR STRENGTHENED BACKUP PRACTICES - CHILE

trendTIC - Digitalization in personal and professional life has increased exposure to risks associated with data loss. In Chile, cybercrimes have shown an upward trend in recent years, driven by the growth of e-commerce and the intensive use of personal devices to store critical data. According to the Chilean Investigative Police (PDI), through its Cybercrime Investigation Brigade, crimes associated with digital fraud, identity theft, and unauthorized access to systems have increased in recent years, especially those linked to social engineering, highlighting a more vulnerable environment for users and organizations.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 2, 2026

BRAZIL ADVANCES IN CYBER DEFENSE AND HUMAN RISK MANAGEMENT GAINS STRATEGIC PROMINENCE IN THE NEW SECTOR MAPPING - BRAZIL

Security Magazine - The launch of the mapping conducted by market professionals in partnership with MITI (Markets, Innovation & Technology Institute) — responsible for the Map of the Brazilian Cyber Defense Ecosystem — marks a new moment for the technology and security sector in Brazil. The initiative organizes, structures, and gives visibility to an ecosystem that had been growing rapidly but still lacked a consolidated vision of its players, competencies, and strategic gaps.

ECONOMY – CENTRAL BANK STUDIES REGULATION OF ARTIFICIAL INTELLIGENCE AND QUANTUM CRYPTOGRAPHY TO INCREASE SECURITY IN THE FINANCIAL SECTOR AND COMBAT FRAUD - BRAZIL

Reporter Maceio - The Brazilian Central Bank (BC) is delving into studies related to the regulation of emerging technologies, such as Artificial Intelligence (AI) and quantum computing, with an emphasis on cybersecurity. This initiative was highlighted by Carlos André de Melo Alves, coordinator of the BC's Financial System Regulation Department. Carlos André stated that the institution is in a process of learning and dialogue with other regulators, especially regarding quantum cryptography.

BRAZIL'S INTERNET STEERING COMMITTEE UPDATES GUIDE AGAINST ONLINE SCAMS

Diario do RN - The Center for Studies, Response and Treatment of Security Incidents in Brazil (CERT.br), a group dedicated to thinking about security within the Brazilian Internet Steering Committee (CGI.Br), has launched an updated version of its security guide, with two volumes dedicated to education against online scams and fraud. They highlight, in easy and accessible language, the dynamics of the most relevant scams currently being used, detailed and based on previous research, metrics related to internet advertising and the use of leaked data.

THE EU AND LATIN AMERICA AND THE CARIBBEAN STRENGTHEN THEIR COLLABORATION ON CYBERSECURITY AND SECURE CONNECTIVITY

EEAS - Over three days of intensive sessions, partners from the European Union and Latin America and the Caribbean addressed the priority topics of their shared digital agenda, highlighting: Cyber resilience and incident response: Through the EU-LAC Cyber-SHIELD program, progress was made in cooperation to strengthen the security of critical systems and the capacity to respond to cyber threats. Public-private partnerships in cybersecurity: Matchmaking sessions were organized to foster collaborations between the public and private sectors, strengthening secure connectivity in the region. Secure connectivity and advanced technologies: Joint initiatives in secure 5G and reliable satellite connectivity were promoted, seeking to ensure resilient and reliable digital networks.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 2, 2026

CISA URGES ENDPOINT MANAGEMENT SYSTEM HARDENING AFTER CYBERATTACK AGAINST US ORGANIZATION - USA

CISA - CISA is aware of malicious cyber activity targeting endpoint management systems of U.S. organizations based on the March 11, 2026 cyberattack against U.S.-based medical technology firm Stryker Corporation, which affected their Microsoft environment.1 To defend against similar malicious cyber activity, CISA urges organizations to harden endpoint management system configurations using the recommendations and resources provided in this alert. CISA is conducting enhanced coordination with federal partners, including the Federal Bureau of Investigation (FBI), to identify additional threats and determine mitigation actions.

PALO ALTO NETWORKS ANNOUNCES INNOVATIONS TO STRENGTHEN CYBERSECURITY IN THE ERA OF ADVANCED AI

Summa Magazine – At a time when the adoption of artificial intelligence, the use of autonomous agents, and the reliance on browsers as a work platform are transforming digital environments, four innovations were presented that address new and growing security needs. These latest solutions offer ways to strengthen operational resilience, protect human and non-human identities, prevent critical disruptions, and securely enable AI-based work models. For organizations in Latin America, where accelerated digitalization continues to expand, these capabilities represent an opportunity to strengthen infrastructure and prepare businesses for increasingly complex scenarios.

ONLY 5% OF ORGANIZATIONS FULLY TRUST CYBERSECURITY VENDORS, REVEALS SOPHOS

tiinside - In Sophos' independent global study on the relationship between companies and cybersecurity solution providers, 95% of respondents stated they do not have full confidence in their suppliers. Based on responses from 5.000 organizations in 17 countries, including Brazil, the study examines one of the most urgent and neglected needs in cybersecurity: trust. The report Cybersecurity Trust Reality 2026 This is one of the most comprehensive studies ever conducted on trust in cybersecurity and its impact on operational risk and executive board decision-making. The survey reveals a critical challenge faced by CISOs: trust in cybersecurity vendors is fragile, difficult to measure, and increasingly decisive in shaping organizations' risk posture, both at the operational and strategic levels.

AI WILL DRIVE SCALABLE CYBERATTACKS IN 2026: GOOGLE CLOUD

Mexico Business Review - By 2026, AI will transition from an exceptional tool to the operational norm for cyber adversaries, enabling automated attacks at a massive scale, says Google Cloud Security. This transformation, alongside the exploitation of hypervisors and critical supply chains, redefines security priorities for enterprises in Mexico and the Latin American region. "Organizations must be prepared for the threats and the adversaries that leverage AI," says Jon Ramsey, Vice President and General Manager, Google Cloud Security. This warning is relevant for the Latin American market, where the rapid adoption of AI agents without robust controls creates significant risks for compliance and the protection of intellectual property.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 2, 2026

WHY THE AI ECONOMY CAN'T RELY ON A SINGLE DIGITAL SUEZ

WEF - When several undersea cables were severed in the Red Sea in early 2024 – initially attributed to accidental damage but later suspected to be connected to Houthi attacks on shipping off Yemen – the impact was felt almost instantly. Latency between Europe, Asia and Africa spiked overnight. Cloud services slowed. Financial transactions faltered. Hundreds of companies and millions of users experienced disruptions without ever knowing why. For data centres and markets, the impact was immediate. For governments, it should have been a wake-up call. This incident was only one of the suspected sabotage attacks on undersea cables, with at least 11 in the Baltic Sea between 2023 and 2024 and multiple incidents in the waters around Taiwan in 2025. Not to mention the dozens of accidents occurring from fishing and unintentional anchor damage to the nearly 600 worldwide undersea cables.

DEMOCRATIZING CYBERCRIME: HOW SOPHISTICATED AI SYSTEMS ARE EMPOWERING A NEW GENERATION OF CYBERCRIMINALS

Global Initiative - AI is once again in the news for the wrong reasons, with recent developments at two major companies – Anthropic and OpenAI – introducing an unprecedented cybersecurity vulnerability into global digital infrastructure. On 26 March, Anthropic accidentally leaked internal documents detailing a new tool named 'Claude Mythos', described by the company as 'by far the most powerful AI model we've ever developed'. The unreleased materials, made publicly accessible in error, also revealed that Anthropic is seriously concerned about the system's 'near-term risks in the realm of cybersecurity'. In response to the incident, a company spokesperson said Anthropic was proceeding with 'extra caution' ahead of the release of Mythos. Nevertheless, the news sent alarm bells ringing across the cybersecurity industry, as concerns were raised that the development of offensive AI capabilities – used to plan or execute malicious activity – is outpacing the development of defensive technology.