DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 30, 2026

DIGI AMERICAS ALLIANCE MEMBERS

Apple · aws · Batuta · CHECK POINT · CISCO · CLOUDFLARE · CROWDSTRIKE · fluid attacks we hack your software

Google · kriptos · LUMU · netskope · paloalto NETWORKS

Resecurity · Schneider Electric · SISAP Sistemas Aplicativos · SOPHOS · tenable · Trellix · TREND MICRO

COLOMBIA PREPARES SPECTRUM ALLOCATION TO IMPROVE RURAL CONNECTIVITY

bnamericas - Colombia is preparing a process to allocate radio spectrum to local stakeholders, aiming to expand residential fixed internet connectivity in rural and remote areas of the country. The initiative involves granting local use permits for the 900MHz band, considered optimal for rural environments due to its propagation characteristics, with the goal of expanding internet access in these areas. The Ministry of Information and Communications Technologies (ICT) is evaluating the allocation of spectrum to connectivity communities and telecommunications network and service providers that, by June 30, 2025, had fewer than 30,000 connections.

CHILE JOINS THE LATIN AMERICAN AND CARIBBEAN CYBERCAPABILITIES CENTER

Segurilatam – The Chilean National Cybersecurity Agency (ANCI) has announced its official incorporation as a new member of the Latin America and Caribbean Cyber Competence Centre (LAC4). This international center promotes cooperation and joint learning in cybersecurity between Latin America, the Caribbean, and Europe. LAC4 Director Liina Areng highlighted that Chile's incorporation represents a significant step in strengthening digital security in South America and reflects the European Union's ongoing commitment to developing a more secure digital environment in the region.

EXPERTS WARN THAT THE HEALTHCARE SECTOR IS AN EASY TARGET FOR HACKERS IN BRAZIL

Viva - This Wednesday, January 28th, Brazil celebrates International Data Protection Day in a context of increasing digital vulnerability. Established in 2006, the date marks the anniversary of Council of Europe Convention 108 — the first international treaty to guarantee privacy, signed in 1981. However, decades after this global commitment, national cybersecurity faces challenges. Data from Check Point's Global Cyberattack Statistics Report shows a 38% increase in online criminal attacks in December alone, a rate that exceeds the defense capacity of most organizations.

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 30, 2026

AGREEMENT BETWEEN BRAZIL AND THE EUROPEAN UNION ON PERSONAL DATA BOOSTS SCIENTIFIC AND DIGITAL COOPERATION

Radar Digital Brasil - The Brazilian government and the European Union have announced the reciprocal recognition of the equivalence of the high and reliable standards adopted by their systems for the protection of personal data and privacy. The decision establishes a legal framework of trust for the international transfer of personal data between Brazil and the European Union, ensuring the protection of rights and legal certainty whenever the circulation of data is necessary for economic activities, the provision of services, opportunities for cooperation in science, technology, scientific research, and the use of digital platforms with international operations.

CYBERSECURITY RISKS WILL MULTIPLY IN 2026; CYBERCRIMINALS ARE FOCUSING ON MEXICO AS A PRIORITY TARGET

Diario Noticias Web - The president of the Board of Directors of Interdisciplinary Projects and Supplies (PSI-Mexico) and researcher at the National Polytechnic Institute, Ezequiel Aguiñiga Tinoco, pointed out that 2025 was characterized by the accelerated adoption of artificial intelligence in the world, which is transforming productivity; and for this 2026, the risk landscape in cybersecurity will multiply significantly, especially in our country.

CYBERSECURITY IN LATIN AMERICA 2025: CRITICAL GAPS AND THE IMPACT OF AI

ImpactoTIC - Latin America and the Caribbean show modest progress in cybersecurity, but institutional gaps persist that jeopardize public services and digital economies. According to the IDB-OAS Cybersecurity Report 2025, only 13 countries have the capacity to implement their national strategies, facing new challenges from the malicious use of AI.

INTERNATIONAL DATA PRIVACY DAY: WHY IT'S KEY IN THE DIGITAL AGE

La 100 - On January 28, International Data Protection Day is commemorated, a date linked to the opening for signature of Convention 108 of the Council of Europe. This instrument was the first global pact on privacy and marked the beginning of international standards on the protection of personal data. The Inter-American Institute of Human Rights (IIDH) has been an Observer Member of the Consultative Committee of Convention 108 since 2021 and has offered the International Diploma Program “The Human Right to Privacy and the Protection of Personal Data” since that same year. The third edition was planned for the second half of 2023.

CYBER CENTRE RELEASES RANSOMWARE THREAT OUTLOOK 2025 TO 2027 - CANADA

Government of Canada - Today, the Canadian Centre for Cyber Security (Cyber Centre), part of the Communications Security Establishment Canada (CSE), released its Ransomware Threat Outlook 2025 to 2027, its latest assessment of ransomware threats facing Canada. The modern ransomware landscape is a highly sophisticated and interconnected ecosystem that is constantly evolving. Understanding current and emerging trends is critical to helping Canadians better prepare for and mitigate ransomware risks.

INSIGHTS

JANUARY 30, 2026

LATIN AMERICA CYBER SECURITY MARKET ANALYSIS: GROWTH, TRENDS, AND FORECAST (2026-2034)

Vocal Media - The digital landscape in Latin America is evolving at breakneck speed, but this rapid technological expansion has a dark side. Recent studies indicate that organizations in the region now face an average of 2,716 cyber attacks per week, a figure that stands 39% higher than the global average. As businesses scramble to protect their digital assets, the Latin America cybersecurity market has become a critical focal point for investors, governments, and enterprise leaders alike.

HEALTHCARE CYBERSECURITY MARKET TO REACH US$ 78.78 BILLION BY 2033 AT 16.5% CAGR; NORTH AMERICA LEADS WITH 41% SHARE | KEY PLAYERS PALO ALTO NETWORKS, CROWDSTRIKE, CHECK POINT

openPR - The healthcare cybersecurity market reached US$ 20.01 billion in 2024 and is expected to reach US$ 78.78 billion by 2033, growing at a CAGR of 16.5% during the forecast period 2025-2033. Market growth is driven by the rapid digitalization of healthcare systems, increasing adoption of electronic health records and connected medical devices, and the rising frequency of cyberattacks targeting healthcare data. Healthcare organizations are investing heavily in advanced cybersecurity solutions to protect sensitive patient information, ensure regulatory compliance, and maintain operational continuity. The market is high in North America, supported by stringent data protection regulations and advanced healthcare IT infrastructure, while Europe follows with strong compliance-driven adoption. Asia-Pacific is emerging as a high-growth region due to expanding healthcare digitization, growing awareness of data security risks, and increasing investments in cybersecurity frameworks across hospitals and healthcare networks.

APTS, CYBERCRIMINALS WIDELY EXPLOITING WINRAR VULNERABILITY

Security Week - Tracked as CVE-2025-8088, the high-severity bug was patched on July 30, after being exploited in the wild as a zero-day by the Russia-linked hacking group named RomCom (also known as Storm-0978, Tropical Scorpius, and UNC2596). The issue is described as a path traversal flaw in WinRAR for Windows that can be abused for arbitrary code execution using crafted archive files. According to GTIG, APTs and cybercrime groups have exploited the security defect via malicious files hidden within the Alternate Data Streams (ADS) of a decoy file inside an archive.

AI-POWERED POLYMORPHIC ATTACK LURES VICTIMS TO PHISHING WEBPAGES

CSO - AI-fueled attacks can transform an innocuous webpage into a customed phishing page. The attacks, revealed in a research from Palo Alto Networks' Unit 42, are clever in how they combine various obfuscation techniques. The combination though can be lethal, difficult to discover, and represent yet another new offensive front in the use of AI by bad actors to compromise enterprise networks. The attack starts with an original and ordinary webpage then attackers add client-side API calls to LLMs that can dynamically generate malicious JavaScript code in real time. This polymorphic technique is dangerous for several reasons.