DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2025

DIGI AMERICAS ALLIANCE MEMBERS

NATIONAL ALLIANCE LAUNCHED TO PREVENT INTERNET SCAMS - BRAZIL

RadioAgência - The Ministry of Justice and Public Security and the Brazilian Federation of Banks have launched a national alliance to combat digital banking fraud. The goal is to create measures to prevent online scams and improve services for victims. The government will work with banks, telephone companies, online retailers and social networks to develop security measures. Every two months, a steering committee will evaluate the progress of the proposals.

SELLING IRIS DATA FOR AI: DIGITAL SECURITY RISKS - BRAZIL

FolhaDeCianorte - The commercialization of biometric data, such as iris scans, to Artificial Intelligence (AI) companies has raised concerns about digital security and privacy. In Brazil, around 500,000 people had their irises scanned in exchange for cryptocurrencies through the Worldcoin project, which was suspended by the government due to regulatory issues. The collection and storage of this data poses a high risk because, unlike passwords, the iris is immutable and, if compromised, can be exploited by cybercriminals.

GOVERNMENT OF SERGIPE STRENGTHENS CYBERSECURITY IN PARTNERSHIP WITH THE FEDERAL GOVERNMENT - BRAZIL

f5news - Last weekend, representatives of the Sergipe Information Technology Company (Emgetis) were in Brasília (DF) for a strategic meeting with the Institutional Security Office of the Presidency of the Republic (GSI/PR). The meeting, held at the Planalto Palace, marked the urgent adhesion of the Government of Sergipe to the Federal Network for Cyber Incident Management, strengthening the state's capacity to respond to and prevent digital threats.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2025

DISCUSSION ON THE ROLE OF ARTIFICIAL INTELLIGENCE IN PUBLIC SAFETY AND CYBERSECURITY IS HELD - MEXICO

TallaPolitica - With the aim of advancing the construction of a regulatory framework on Artificial Intelligence (AI), the Commission for Analysis, Monitoring and Evaluation on the application and development of AI in Mexico, chaired by Senator Rolando Zapata Bello, held the second discussion with specialists in the field, under the theme "Roles of AI in public safety, cybersecurity and risk management."

PRI PROMOTES REFORM TO PROTECT MEXICO AGAINST CYBERATTACKS

Heraldo de Mexico - Faced with the increase in cyber attacks, digital scams and identity theft in Mexico, the senator of the Institutional Revolutionary Party (PRI), Alejandro Moreno Cárdenas, presented an initiative to strengthen the country's digital security. The national leader of the PRI also establishes the creation of a General Law on Cybersecurity, which will regulate the protection of data and computer systems, defining clear responsibilities for the public and private sectors.

WITH APPROVAL OF AI CONPES, THE COUNTRY ALREADY HAS A PUBLIC POLICY FOR THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE - COLOMBIA

trendTIC - The approval of the National Artificial Intelligence (AI) Policy by Conpes is the result of the joint and committed work of the ICT and Science, Technology and Innovation Ministries, the National Planning Department, the Administrative Department of the Presidency of the Republic, and the Ministries of Commerce, Industry and Tourism; Education and Labor. Through this Public Policy, the Colombian State is committed to developing concrete actions to take advantage of this technology in a strategic and sustainable way, understanding that it has the potential to boost productivity, innovation and decision-making.

CYBERSECURITY FRAMEWORK LAW: HOW AND WHICH COMPANIES IT AFFECTS - CHILE

Bad Thing - The National Cybersecurity Agency will define in March the two groups that must follow the obligations in this matter: essential services and vital operators. Both groups must prevent, report and resolve cybersecurity incidents in their companies, or face fines of up to 40 thousand UTM.

DEEPSEEK BLOCKED IN SEVERAL COUNTRIES DUE TO CYBERSECURITY RISKS

MegaNews - The artificial intelligence DeepSeek, developed in China, has generated great controversy worldwide in recent weeks. Several countries have decided to restrict its use due to concerns about data protection and national security. South Korea was the latest to join the list on February 15, when it suspended the local service of the application for alleged violations of its privacy laws.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2025

FIND OUT HOW MANY THREATS ARE BLOCKED PER SECOND: SOCIAL NETWORKS PREFERRED BY SCAMMERS

Forbes - Social media, AI, and human trust fueled a record year for advanced scams and personal data loss. The [Gen] report reveals a surge in online threats to close out a record-breaking 2024, with 2.55 billion cyberthreats blocked between October and December, equivalent to 321 threats per second.

THESE ARE THE RISKS TO WHICH YOU EXPOSE YOUR PERSONAL DATA ON DIGITAL PLATFORMS

La Republica - One of the biggest challenges facing the new digital generations, following the evolution of tools such as artificial intelligence, is to protect users' private information. Although the digitalization of everyday life accelerated work processes, it is also true that it placed, almost on a silver platter, users' personal information at the mercy and will of digital companies, a breeding ground for possible fraud.

WHAT A NEW PRESIDENCY MEANS FOR GLOBAL CYBERSECURITY—AND FOR SMES - USA

Forbes - As a cybersecurity leader dedicated to safeguarding small- and medium-sized enterprises (SMEs) from cyber threats, the shifting sands of the cybersecurity landscape are always top-of-mind. The recent election of Donald Trump as President of the United States introduces new dynamics that could significantly impact global cybersecurity practices.

CYBER CONSPIRACY MODERNIZATION ACT PROPOSED, CYBER EXPERT WEIGHS IN - USA

Security Magazine - A bipartisan bill introduced by Senator Mike Rounds (R-SD) and Senator Kirsten Gillibrand (D-NY) aims to increase punishment for cybercrimes. This bill, the Cyber Conspiracy Modernization Act (CCMA), seeks to modify the Computer Fraud and Abuse Act (CFAA) in order to enact a penalty for conspiracy and strengthen penalties for offenders. This bill was introduced in as a set, joined by the Providing Individuals Various Opportunities for Technical Training to Build a Skills-Based Cyber Workforce Act of 2025 (Cyber PIVOTT Act), which would offer scholarships for students and professionals in cyber-related fields.

THE AI HYPE FRENZY IS FUELING CYBERSECURITY RISKS

Forbes - The artificial intelligence gold rush has reached a fever pitch. Companies are throwing billions—no, trillions—at AI projects, slapping the "AI-powered" label on everything from email filters to coffee makers. AI is no longer just a technology; it’s a buzzword, a marketing gimmick and a financial frenzy all rolled into one. We’ve warned about this before. AI is not magic—it’s just software with access to massive datasets, making predictions based on patterns. But the relentless hype machine has distorted reality, and now we’re facing the consequences. This unchecked AI mania is driving expected catastrophic cybersecurity risks—some of which may be irreversible.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2025

THE HIDDEN CYBERSECURITY CRISIS: HOW GENAI IS FUELING THE GROWTH OF UNCHECKED NON-HUMAN IDENTITIES

Security Boulevard - Generative AI continues its promises of revolutionizing industries and transforming everything from customer service to software development. Behind the excitement, organizations continue to struggle to identify and validate applicable use cases for GenAI that bring real business benefits. At the same time, industry leaders and social pundits continue to beat their loud revolutionary GenAI drums, enticing employees to frantically play with every new AI tool or risk losing professional and personal relevance. By doing so, they unknowingly grant access to APIs, service accounts, tokens and other NHIs which in in turn grant these applications extensive ecosystem permissions and access. As a result, a growing cybersecurity crisis is emerging — one that many organizations are unprepared to handle. GenAI is accelerating the unchecked growth of NHIs, fueling a new wave of cyberthreats.

THE FOUNDATION OF MODERN SOFTWARE DEVELOPMENT IS UNDER RISING CYBER ATTACK

NBC New York - Organizations are seeing a rise in cybersecurity attacks against application programming interfaces, and they aren't always prepared to defend themselves. As the foundation of modern software development, APIs facilitate communication between apps and fuel digital transformation, but this critical role has broadened the attack surface, making APIs a prime target for cybercriminals. The average cost to remediate API incidents was $591,400 in the U.S. In sectors such as financial services, the average was $832,800.