DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 27, 2025

DIGI AMERICAS ALLIANCE MEMBERS

FORCIC CYBERSECURITY AND CYBERCRIME PROGRAM - ARGENTINA

Abogados.com.ar - The Cybersecurity and Cybercrime Investigation Strengthening Program (ForCIC), run by the Cybercrime and Cyber Affairs Directorate, was created as a result of the increase in cybercrimes and the number of people affected by them, and especially considering the transnational nature of these crimes. With the aim of combating them at the federal and international level, the ForCIC program assumed the responsibility of coordinating, assisting and providing advice on digital infrastructure security techniques and on investigation techniques in cybercrimes or crimes that use technology.

ABES: BRAZIL NEEDS THE NATIONAL CYBERSECURITY AGENCY YESTERDAY

Convergencia Digital - At a press conference held this Thursday, February 20, for the launch of the 2025 Regulatory Agenda of the Brazilian Association of Software Companies (ABES), the entity's vice president, Andriei Gutierrez, was categorical: If Brazil has to create a new regulatory agency, it should be dedicated to Cybersecurity. ABES rules out an agency for Artificial Intelligence and argues that current regulatory agencies are capable of regulating and monitoring the use of technology in their sectors.

THE GENERAL DATA PROTECTION LAW (LGPD) IN BRAZIL: CHALLENGES AND IMPACTS ON CONSUMER RELATIONS IN THE DIGITAL ENVIRONMENT

Legal Content - The protection of personal data is emerging as one of the main regulatory challenges of the digital age, amid a scenario of technological advances that have transformed the collection and use of individual information into strategic resources for companies and institutions. In this context, privacy, once perceived as an individual right limited to the sphere of intimacy, acquires a collective and global dimension, imposing the need for legislation that harmonizes innovation, security and respect for fundamental rights. In Brazil, the General Data Protection Law (LGPD) emerges as a regulatory framework that aligns the country with international practices, promoting greater balance in the relationships between data subjects and processing agents (BRASIL, 2018).

PANAMA CANAL AND U.S. SOUTHERN COMMAND TO COOPERATE ON CYBERSECURITY

PortalPortuario - The Panama Canal and the United States Southern Command (USSOUTHCOM) signed a Cyber Cooperation Agreement with the aim of strengthening digital security and ensuring the operational continuity of critical infrastructure in the face of emerging cyber threats. The agreement establishes a collaborative framework to improve capabilities in key areas such as cybersecurity training, supply chain security, information exchange, and technical assistance.

GR LAUNCHES THE NATIONAL CYBERSECURITY CAMPAIGN 2025: “SAFE INTERNET FOR ALL” - MEXICO

afmedios - Within the framework of the National Security Strategy, the National Guard has launched the national Cybersecurity 2025 campaign “Safe Internet for All”, with the aim of raising awareness among the population about the safe and responsible use of information technologies, as well as encouraging the reporting of cybercrimes.

CYBERCRIMINALS USE AI ON VERIFIED YOUTUBE ACCOUNTS TO STEAL DATA AND CARRY OUT FINANCIAL ATTACKS

infobae - Cybersecurity researchers have detected a new digital threat method under the formula of self-deception or 'Scam-Yourself', thanks to which cybercriminals compromised a verified YouTube account with 110,000 subscribers to host a video generated by Artificial Intelligence (AI) containing 'malware' with the aim of executing financial frauds. The self-deception formula consists of pressuring users and psychologically manipulating them into installing and executing malicious code on their computers, which hijacks their user accounts, with their names and credentials, and carries out financial frauds.

U.S. CHAMBER CALLS FOR PUBLIC-PRIVATE, INTERNATIONAL COLLABORATION ON POST-QUANTUM CYBERSECURITY

Inside Cybersecurity - The U.S. Chamber of Commerce wants policymakers to prioritize engaging with the private sector and international allies to mitigate the cybersecurity risks associated with quantum computing, while federal agencies work toward implementing quantum-resistant encryption on their networks. “Quantum computing will render many encryption methods obsolete. The time to address this threat is now,” the Chamber says in a set of guiding principles for policymakers published on Feb. 19.

WHAT MICROSOFT’S MAJORANA 1 CHIP MEANS FOR QUANTUM DECRYPTION

Security Week - The potential power of quantum computing is difficult to imagine, but it will revolutionize society and science. When combined with AI, each technology will help improve the other. So, at some point, advances in AI and quantum computing will become better and faster – the combination will become a continuing and accelerating virtuous cycle. But before the major promise of quantum will come the first known cyber threat: the ability to decrypt the PKE that makes computing and the internet workable.

INSIGHTS

FEBRUARY 27, 2025

SEC TARGETS DIGITAL SCAMS WITH NEW CYBER AND EMERGING TECHNOLOGY UNIT - U.S.

Finance Magnates - The rise of digital fraud and financial cybercrime has prompted the Securities and Exchange Commission (SEC) to take decisive action. The agency announced the formation of the Cyber and Emerging Technologies Unit (CETU), a specialized task force designed to crack down on cyber-related misconduct and protect retail investors from evolving digital threats.

EUROPEAN COMMISSION UNVEILS CYBERSECURITY BLUEPRINT TO STRENGTHEN EU CYBERSECURITY AND CRISIS COORDINATION

Industrial Cyber - The European Commission unveiled on Monday a proposal aimed at ensuring a robust and efficient response to large-scale cyber incidents, thereby enhancing EU cyber crisis coordination. The updated cybersecurity blueprint refines the comprehensive EU framework for Cybersecurity Crisis Management, detailing the roles of relevant EU actors throughout the entire crisis lifecycle. The draft Council Recommendation on the EU Blueprint for cybersecurity crisis management also seeks to present the EU framework in a clear, straightforward, and accessible manner.

IN-DEPTH ANALYSIS OF THE CYBERSECURITY AS A SERVICE CSAAS MARKET – SEGMENTATION, MARKET DYNAMICS, RECENT DEVELOPMENTS

Newswires - The Cybersecurity as a Service (CSaaS) market was valued at USD 23.55 billion in 2023 and is projected to grow from USD 25.36 billion in 2024 to USD 45.91 billion by 2032, reflecting a compound annual growth rate (CAGR) of 7.7% during the forecast period from 2024 to 2032. The cybersecurity as a service (CSaaS) market is experiencing significant growth, driven by the increasing need for robust security solutions in the face of rising cyber threats and the growing adoption of cloud-based infrastructure. CSaaS refers to the provision of cybersecurity services via the cloud, offering businesses scalable, flexible, and cost-effective protection against a wide range of cyber risks.

A PROACTIVE BLUEPRINT FOR MODERN CYBERSECURITY

Forbes - Cybersecurity has never been more critical—or more challenging—than it is today. Organizations face a constant barrage of cyber threats that evolve at dizzying speed, while most security teams juggle an ever-growing patchwork of disparate tools. In this high-stakes environment, the concept of Continuous Threat Exposure Management is emerging as a pivotal strategy for identifying, prioritizing, and neutralizing potential vulnerabilities before they escalate into full-blown incidents. Rather than relying solely on post-incident cleanup or one-off assessments, CTEM emphasizes a continuous, proactive cycle that unifies detection and prevention under one strategic umbrella.

3.9 BILLION PASSWORDS STOLEN—INFOSTEALER MALWARE BLAMED

Forbes - Considering just how many infostealer malware warnings have been issued recently, from macOS-specific threats, to those targeting a broad sweep of Gmail and Outlook email users, there can be little doubting that cybercrime actors are coming for your passwords. Now the true reach of the infostealer malware threat has been laid bare by a threat intelligence agency which specializes in leveraging dark web data, and the picture it paints is a scary one. Here’s what you need to know.

IIOT CYBERSECURITY: MINIMIZING RISK WITH THE CIA TRIAD

IoT For All - Organizations have a growing need for data collection and analytics. As a result, many are adopting cutting-edge Industrial Internet of Things (IIoT) technologies, such as connected sensors and cloud-based software. IIoT joins hardware and software in a connected system, allowing remote monitoring, automated alerts, and integration with computers and mobile devices. The adoption of IIoT supports innovative maintenance and reliability solutions, connecting with supervisory control and data acquisition (SCADA) systems and monitoring the condition of programmable logic controllers (PLCs) in real time. However, connecting manufacturing plants to the internet also exposes them to increased risks of cyberattacks.