DIGI AMERICAS ALLIANCE MEMBERS

CONGRESS CREATES PARLIAMENTARY FRONT TO PROMOTE DEBATES AND STRENGTHEN DIGITAL SECURITY IN THE COUNTRY - BRAZIL

Brazil, pais digital - The rise in cybercrime is a threat that concerns all countries in the world, with dramatic consequences that put private companies, government institutions and the lives of citizens at risk. Brazil, one of the countries most targeted by cybercriminals, recorded more than 103 billion attempted cyberattacks in 2022, an increase of 16% compared to the previous year. A study by INCC (National Institute for Combating Cybercrime) revealed that data breaches in Brazil generated direct, indirect and induced losses of R$2.3 trillion in 2024, which represents a loss of 18% in annual GDP.

INVESTMENTS IN ICT IN BRAZIL EXCEEDED R$500 BILLION

Convergencia Digital - IT sector investments jumped from US$49.8 billion in 2023 to US$58.6 billion in 2024, with emphasis on the advancement of artificial intelligence (AI), business digitalization and the modernization of cloud infrastructures and cybersecurity, which means a significant growth of 13.9% in 2024, while the global average was 10.8%. If IT + Telco are added, the amount was US$90 billion, reveals the study Brazilian Software Market Study - Panorama and Trends 2025, released by the Brazilian Association of Software Companies (ABES).

LNCC REINFORCES COMMITMENT TO CYBERSECURITY AT THE OPENING OF THE SECOPS SUMMIT 2025 IN PORTO ALEGRE - BRAZIL

gov.br - On the morning of last Wednesday (19), the SecOps Summit 2025 began at the PUCRS Events Center, in Porto Alegre, with the participation of Bruno Alves Fagundes, head of the Systems and Networks Support Service (SERED) of the National Laboratory for Scientific Computing (LNCC/MCTI). Representing the institution, Fagundes highlighted the importance of LNCC in promoting scientific research and offering a high-performance computing platform, with an emphasis on information security, validated by ISO 27001 certification.

DIGI AMERICAS LATAM CISO

INSIGHTS

MARCH 27, 2025

DIGITAL TRANSFORMATION AGENCY: KEY TECHNOLOGY PROJECTS FOR 2025 - MEXICO

elciudadano - The Digital Transformation and Telecommunications Agency is preparing for a crucial year in 2025, with the launch of several projects that seek to boost digitalization and cybersecurity in Mexico. This was announced by José Antonio Peña Merino, head of the agency, who detailed the initiatives that will shape the future of the sector in the coming years.

MEXICAN AUTHORITIES RECOMMEND MEASURES FOR CRYPTOCURRENCY USE

Prensa Latina - A statement from the Secretariat of Security and Citizen Protection (SSPC) warns about the dangers associated with digital currencies, which are characterized by being volatile, costly to transact, and unstable. According to the source, among the scams most commonly used by cybercriminals are fake websites, which generally solicit ongoing investments, promise large returns, and use fake testimonials from satisfied customers.

THE PRESIDENT'S HACK HIGHLIGHTS THE VULNERABILITY OF ALL MEXICAN USERS TO CYBERATTACKS - MEXICO

infobae - For context, Mexican President Claudia Sheinbaum reported during her morning press conference on Monday, March 17, 2025, that one of her cell phones and one of her email accounts had been compromised by cybercriminals. The president clarified that the compromised number corresponds to one she used during her election campaign and no longer uses. She also assured that her official accounts have adequate security measures. Sheinbaum also indicated that the Digital Transformation Agency is investigating the incident, although those responsible for the cyberattack have not yet been identified.

INDOTEL PRESIDENT AND MAYOR OF NEW YORK DISCUSS CYBERSECURITY AND DIGITAL TRANSFORMATION - DOMINICAN REPUBLIC

presidencia.gob.do - The president of the Board of Directors of the Dominican Telecommunications Institute (Indotel), Guido Gómez Mazara, met with the mayor of New York City, Eric Adams, where they discussed key topics related to cybersecurity and the use of technological solutions to improve citizens' quality of life.

DIGI AMERICAS LATAM CISO

INSIGHTS

MARCH 27, 2025

CENTRAL BANK ACCELERATES STRATEGY AGAINST CYBER RISKS - BRAZIL

portalin - The growing threat of cyber risks is on the radar of the Central Bank (BC), which has made the topic a strategic priority to protect the financial sector. This year, the BC set up a specialized team to monitor incidents reported by institutions and intensified the schedule of the “IT Map” – a tool to identify technological vulnerabilities and improve the security of operations. The goal is to ensure that, by the beginning of next year, all supervised institutions are incorporated into the project, which already covers around 70% of the sector. Among the areas of attention are the use of Artificial Intelligence and APIs (acronym in English for Application Programming Interface) in the consumption of financial services.

FIGHT AGAINST ORGANIZED CRIME: PARAGUAY AND COLOMBIA STRENGTHEN MILITARY ALLIANCE

adndigital - The Paraguayan and Colombian Armed Forces reaffirmed their close cooperation in security and defense matters, reaching 58 new agreements to combat organized crime and transnational crimes. President Santiago Peña Nieto met with the Commander of the Colombian Armed Forces, Francisco Cubides, in Mburuvicha Róga this Thursday, as part of the Second Round of Talks between senior military commanders from both countries, currently taking place in Asunción.

TRUMP ADMINISTRATION BEGINS SHIFTING CYBERATTACK RESPONSE TO STATES - USA

The Wall Street Journal - The Trump administration wants state and local governments to play a bigger role in protecting water utilities, ports and other critical infrastructure from cyberattacks. In an executive order signed Tuesday, President Trump directed White House senior security advisers to draw up a national resilience plan to protect critical infrastructure that shifts more responsibilities to the state and local level. Trump also called for a review of several executive orders and actions from the Biden administration, including those that establish a whole-of-government approach in managing cyber risks to critical infrastructure.

CHINA’S WORRISOME CYBER PENETRATION IN LATIN AMERICA

Dialogo Americas - Attacks from China state-sponsored hacker groups in Latin America have not only increased in recent years but have also become more sophisticated. According to cybersecurity reports and experts, the People’s Republic of China (PRC) is considered the main state sponsor of cyberattacks in the region, using cyber operations to promote its economic and diplomatic interests in the region, often targeting critical infrastructure and government networks.“China facilitates cyberattacks in Latin America to achieve its political, economic, and intelligence gathering objectives,” Belisario Contreras, senior director of Global Security and Technology Strategy at Venable LLP and coordinator of the Digi Americas Alliance, a network of organizations dedicated to cybersecurity in the Americas, told Diálogo.

DIGI AMERICAS LATAM CISO

INSIGHTS

MARCH 27, 2025

INSIGHTS ON AI-ENABLED CYBER-CRIME THROUGH COLLABORATION WITH UC BERKELEY'S CENTER

ITWeb - Over the last year, discussions about Artificial Intelligence (AI)-enabled cyber crime have shifted from speculation about impacts to real-world observations. Malicious actors continue to find ways to harness AI to their advantage, resulting in an increased volume and velocity of threats, keeping the cybersecurity community on their toes. As defenders, having an awareness of AI's impacts on the threat landscape is certainly vital, as is understanding strategies to combat the shifts occurring in the wake of this new technology. Gaining hands-on practice mitigating AI-focused threats is the next crucial step in fighting increasingly sophisticated cybercrime operations.

THE INTERVENTION JOURNEY: A ROADMAP TO EFFECTIVE DIGITAL SAFETY MEASURES

WEF - With the increasing digitization of society, online harms – such as child sexual exploitation, scams, privacy violations and disinformation – are growing in complexity and volume. Many organizations struggle to implement interventions due to limited resources, regulatory complexity and rapidly evolving threats, putting them at risk of legal and reputational consequences. The Intervention Journey: A Roadmap to Effective Digital Safety Measures proposes a detailed plan for how to implement digital safety interventions.