DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 13, 2025

DIGI AMERICAS ALLIANCE MEMBERS

MAP BRINGS TOGETHER THE STATE'S TECHNOLOGY AND CYBERSECURITY DIRECTORS - DOMINICAN REPUBLIC

DiaroDigitalRD - The Ministry of Public Administration (MAP), through the Vice Ministry of Innovation and Technology, brought together directors and those in charge of technology and cybersecurity in the public sector to define the digital transformation strategy and strengthen government efficiency through the use of innovative technologies. The MAP minister, Sigmund Freund, stressed that the digitalization of the State is essential to offer more agile, accessible and transparent services.

INDOTEL PRESIDENT MEETS WITH U.S. DEPUTY ASSISTANT SECRETARY TO STRENGTHEN TIES AND COOPERATION IN CYBERSECURITY - DOMINICAN REPUBLIC

The President of the Board of Directors of the Dominican Institute of Telecommunications (Indotel), Guido Gómez Mazara, met with the Principal Deputy Assistant Secretary of the United States Department of State for the Office of Cyberspace and Digital Policy, Jennifer Bachus, with whom he exchanged strategies to strengthen cybersecurity in the Dominican Republic, in order to have a more robust and secure digital future.

MITIC REPORTS ON PROGRESS IN CYBERSECURITY STRATEGIES AND DIGITAL AGENDA - PARAGUAY

La Nacion - The Ministry of Information and Communication Technologies (Mitic) published its “Annual Report” for 2024 in which it sets out all the actions promoted by this institution during the past year. These include events such as digital identity, technical assistance, among others. One of the fundamental pillars, according to the institution itself, was cybersecurity and in this sense, more than 1,800 incidents were managed and in addition, the National Cybersecurity Strategy was formulated, which extends until 2028 and was developed in collaboration with the Organization of American States (OAS).

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 13, 2025

TRT-RS INTENSIFIES CYBER DEFENSE AGAINST THE ADVANCE OF HACKER ATTACKS - BRAZIL

Labor Court - In recent years, Brazil has been among the main targets of cyberattacks in the world, according to data from specialized reports. This reality has led public and private institutions to reinforce their digital security structures. At the Regional Labor Court of the 4th Region (TRT-RS), this concern is constant, as reported by the director of the Secretariat of Information Technology and Communications (SETIC), André Farias: “Hundreds of thousands of attempts at malicious actions are recorded every day, 24 hours a day, all of which are duly blocked by information security systems”.

CYBERSECURITY REGULATIONS AND TRENDS IN 2025: WHAT TO EXPECT - BRAZIL

Inforchannel - Cybersecurity remains one of the biggest global concerns for 2025, especially given the exponential increase in attacks and data breaches. The scenario is driven by advances in Artificial Intelligence (AI) and the growing sophistication of cybercriminals. On the one hand, AI plays an even more crucial role in protecting companies' digital infrastructures, and on the other, this technology has been widely used by hackers, requiring strong preparation on the part of companies.

“DEVELOPING TECHNOLOGY WITHOUT RESPECTING PRIVACY SHOULD NOT BE AN OPTION,” SAYS DR. PATRÍCIA PECK

ITForum - In an interview with IT Forum, Dr. Patrícia Peck, a digital law specialist and CEO of Peck Advogados, explains: “We are in the process of creating a corporate culture that incorporates the concept of privacy by design, meaning that privacy must be integrated into the design of technological products and solutions.”

CALI CITY HALL STRENGTHENS ITS CYBERSECURITY IN THE FACE OF THE INCREASE IN CYBERATTACKS IN COLOMBIA

Cali City Hall - To ensure the protection of information and prevent cyberattacks, the Cali City Hall, through Datic, has implemented a SOC-SIEM server. This system monitors and protects the district's technological infrastructure, ensuring the integrity of citizens' data. The server operates 24 hours a day, seven days a week, continuously analyzing digital security and generating alerts for technology administrators. This allows for an immediate response to potential threats and reinforces the protection of the District's systems.

MEXICO WILL BE ABLE TO COMBAT CYBERCRIME THROUGH PUBLIC-PRIVATE COLLABORATION

dplnews - Cybercrime represents a growing threat worldwide, and its economic impact could reach 10.5 trillion dollars annually, which highlights the urgent need for a coordinated response between the government and the private sector, said Gonzalo García-Belenguer, director of the Cybersecurity Hub at Tec de Monterrey. The expert said that cyberattacks not only affect the economy, but can also interrupt business operations, create reputation crises and undermine the security of citizens.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 13, 2025

SAFE INTERNET: BUSINESS CYBERSECURITY, CHALLENGES AND STRATEGIES IN THE ERA OF AI

ImpactoTIC - Business cybersecurity is a growing challenge in the face of increasing cyberattacks. Despite increased investments in protection, only 32% of companies are fully confident in their ability to recover. Cyberattacks continue to be the main cause of disruptions to business services, which has prompted companies to strengthen their digital security strategies.

AMERICAS' BOARDROOM PRIORITIES FOR 2025

EY - Uncertainty persists as dynamic forces shape the business context. Boards will adapt their oversight to help management act with intention and confidence. To support transformation, boards will guide portfolio reviews, connect technology security oversight and innovation, and foster talent competitiveness. Boards will prioritize scenario planning based on geopolitical, economic, labor and climate outcomes to build resilience and enable agility.

GOOGLE: CYBER CRIME MESHES WITH CYBER WARFARE AS STATES ENLIST GANGS

ComputerWeekly.com - A report from the Google Threat Intelligence Group depicts China, Russia, Iran and North Korea as a bloc using cyber criminal gangs to attack the national security of western countries. The Google Threat Intelligence Group’s report, Cyber crime: A multifaceted national security threat, says western policymakers should be taking cyber criminality just as seriously as operations conducted by nation states. The report looks at how nation states hostile to the North Atlantic countries, such as Russia, China, Iran and North Korea, are increasingly co-opting cyber criminal groups to forward their geopolitical and economic ambitions. It also looks at the deep societal impact of cyber crime, from economic destabilisation to its toll on critical infrastructure, including healthcare.

HOW THE G7’S NEW AI REPORTING FRAMEWORK COULD SHAPE THE FUTURE OF AI GOVERNANCE

OECD.AI - On 7 February 2025, the OECD launched the reporting framework for monitoring the application of the Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems. This milestone marks a significant advancement in international AI governance, reinforcing the G7’s commitment to ensuring the safe, secure, and trustworthy development, deployment, and use of advanced AI systems.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 13, 2025

THE DIGITAL SHIELD: USING CYBER DIPLOMACY TO STRENGTHEN NATIONAL CYBER RESILIENCE

Georgetown Security Studies - In the modern security environment, unconventional, asymmetric security challenges become increasingly dangerous since adversaries seek cheap and easy ways to confront stronger opponents by exploiting vulnerabilities without engaging in direct, conventional warfare. The cyberspace has emerged as a critical domain which national security systems have to engage with. As cyber-attacks grow more sophisticated, governments recognize that addressing cyber-related issues to strengthen national cyber resilience requires a comprehensive, whole-of-government approach. In this process, cyber diplomacy is a vital aspect of cybersecurity. Cyber diplomacy involves facilitating the development of international cooperation frameworks, norms of behavior, information sharing, and trust-building among nations.

QUANTUM SECURITY MARKET SURGE FUELED BY ESCALATING CYBERSECURITY THREATS DRIVER: A MAJOR CATALYST IN THE EVOLUTION OF THE QUANTUM SECURITY MARKET IN 2025

openPR - How Is the Quantum Security Market Projected to Grow, and What Is Its Market Size?
The scale of the quantum security market has expanded massively in past years. It is set to escalate from a worth of $1.14 billion in 2024 to $1.7 billion in 2025, reflecting a compound annual growth rate (CAGR) of 49.0%. The historic period's expansion has been propelled by the need for advanced simulation and modeling, compounded complexity in automotive systems, heightened emphasis on cybersecurity, collective research efforts, and regulatory pressures.