DIGI AMERICAS ALLIANCE MEMBERS

CYBERSECURITY LAW INITIATIVE PRESENTED - MEXICO

Mexico City Congress - With the goal of strengthening the regulatory framework for personal data protection, the Mexico City Institute for Transparency, Access to Public Information, Personal Data Protection, and Accountability presented the Cybersecurity Law initiative to the local Congress regarding the processing of personal data and information security.

DIGITAL WARFARE: BRAZIL STRENGTHENS CAPABILITIES IN LARGEST GLOBAL CYBER EXERCISE

Defesa em Foco - Between firewalls and simulated attacks, Brazilian military personnel participated in Locked Shields 2025, the largest cyber defense exercise on the planet. Organized by NATO, the training brought together 41 countries in a realistic simulation of digital warfare — and Brazil was the only representative from Latin America. Promoted annually by the NATO Collaborative Cyber Defense Centre of Excellence (CCDCOE), based in Tallinn, Estonia, Locked Shields is considered the most advanced cyber warfare exercise in the world. In 2025, 41 nations joined forces to simulate coordinated digital attacks against critical infrastructure, government networks, and military systems.

BRAZIL AND SPAIN PROMOTE COOPERATION ON DEFENSE AND SECURITY

Forcas Terrestres - With the aim of promoting the Brazilian Defense Industrial Base (BID), the Ministry of Defense, through the Secretariat of Defense Products (Seprod), participated in the 4th International Defense and Security Exhibition of Spain (Feindef). The event took place in Madrid, Spain, from the 12th to the 14th, and brought together 92 international delegations with 601 exhibitors. For the Secretary of Defense Products, Heraldo Luiz Rodrigues, participation in this exhibition was important to foster future partnerships. “Several meetings were held with high-tech companies, mainly in the space and cybernetic areas. All of them showed interest in sharing their knowledge with Brazilian companies, a very strong interest in having a greater share in the defense market”, he said.

THEY ARE INVESTIGATING THE POSSIBLE HACKING OF THE DATA OF 50,000 ARMY PERSONNEL: THE ALERT CAME VIA AN ANONYMOUS EMAIL - ARGENTINA

Infobae - The Argentine Army reported to the Federal Police a possible hacking of personal data belonging to approximately 50,000 members of the force after receiving an anonymous email claiming to contain information about individuals linked to the institution. According to the Army, the initial complaint was filed on May 8 with the Federal Police's Cybercrime Division, and preventive measures have since been adopted to strengthen security in administrative systems.

THE SUPERINTENDENCY OF ELECTRICITY ISSUES CYBERSECURITY REGULATIONS - DOMINICAN REPUBLIC

RCC Noticias- The Superintendency of Electricity (SIE) issued the resolution that puts into effect the "Cybersecurity and Information Security Regulations for the Electricity Subsector in the Dominican Republic," following a public consultation process in accordance with regulations requiring the participation of subsector stakeholders in mandatory guidelines. The SIE reported that the objective of the regulation is to provide the subsector with "tools to safeguard critical technological assets of the National Interconnected Electricity System (SENI)" and to strengthen the response capacity "to cyber threats, which is essential to protect national security, especially in critical infrastructure such as the electrical system."

NEW CYBERATTACK COULD BE "ONE OF THE COUNTRY'S LARGEST DATA BREACHES," SAYS EXPERT - PARAGUAY

abc.com.py - Speaking with ABC Color this Sunday, cybersecurity expert Miguel Ángel Gaspar stated that the cyberattack that affected several state institutions, announced today by the Ministry of Information and Communication Technologies (Mitic), is “one of the largest data breaches in the country.”

LATORRE CONSIDERS STRENGTHENING CYBERSECURITY CAPABILITIES KEY - PARAGUAY

La Nacion - The President of the Chamber of Deputies, Raúl Latorre, indicated that there is a need to continue strengthening cybersecurity capabilities in the country. He noted that this is not a conversation for the future, but rather a conversation about the present that projects into the future. "Artificial intelligence, cybersecurity, the ability to generate peace of mind and security in cyberspace regarding institutional information and economic and financial transactions are fundamental to strengthening our Republic and, in fact, all countries in the world," he stated in a conversation with the press before the start of the session.

DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 15, 2025

AI AGAINST CYBERCRIME: A NEW DEFENSE FOR GUATEMALA

Summa Magazine - Cyberattacks continue to rise in Latin America, to the point where it is the fastest-growing region in terms of disclosed cyber incidents, with an average annual rate of 25% over the last decade, according to the World Bank's "Economics of Security for Emerging Markets" report. Guatemala ranked tenth in terms of disclosed attacks between 2013 and 2024. The most affected sector was manufacturing, followed by public administration.

COMMISSION HEARS OPINIONS FROM EXPERTS ON CYBER DEFENSE AND ATTACKS ON COMPUTER SYSTEMS - GUATEMALA

Congreso.gob.gt - To continue the analysis and discussion of Initiative 6347, the cybersecurity law, the National Security Affairs Committee, chaired by Representative Jorge Mario Villagrán, held a hybrid meeting with the technical advisory panel to advance and improve the content in order to issue the respective opinion for the approval of the bill. The initiative seeks to develop cybersecurity and cyberdefense capabilities, as well as the classification of criminal conduct, to prevent, eradicate, and punish cybercrimes.

GUATEMALA-US THWART CHINA SPY THREAT

Dialogo Americas - Cooperation with the United States has once again proved strategic in countering the growing threat of China-state sponsored cyberattacks in Latin America. Such was the case recently for Guatemala’s Foreign Ministry (MINEX). “Thanks to close collaboration between both countries, these threats were detected, and the necessary measures were taken to stop them and prevent them in the future,” MINEX told Associated Press on April 30. According to MINEX, Chinese hackers infiltrated its computer systems from September 2022 to February 2025. A U.S. Southern Command’s (SOUTHCOM) comprehensive cybersecurity review of Guatemalan security networks led to the detection of the China-based cyber espionage groups.

CONGRESS FACES PRESSURE TO RENEW CYBER INFORMATION-SHARING LAW - USA

Cybersecurity Dive - A coalition of 52 U.S. organizations urged lawmakers on Tuesday to reauthorize a law that protects cyber threat information that businesses share with the federal government. The Cybersecurity Information Sharing Act, which is set to expire on Sept. 30, creates a system for federal agencies to receive threat indicators from companies and share those indicators with other agencies and companies. The law specifies that companies can share threat information with one another without violating antitrust laws and requires agencies to remove personal information before sharing information. It also prohibits the government from using any shared data to regulate companies.

DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 15, 2025

FIVE YEARS LATER: EVOLVING IOT CYBERSECURITY GUIDELINES

NIST - The passage of the Internet of Things (IoT) Cybersecurity Improvement Act in 2020 marked a pivotal step in enhancing the cybersecurity of IoT products. Recognizing the increasing internet connectivity of physical devices, this legislation tasked NIST with developing cybersecurity guidelines to manage and secure IoT effectively. As an early building block, we developed NIST IR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers, which describes recommended activities related to cybersecurity for manufacturers, spanning pre-market and post-market, to help them develop products that meet their customers' needs and expectations for cybersecurity.

RESEARCH ON CYBER SECURITY IN ENTERPRISE CONNECTED DEVICES

Gov.uk - The UK government is concerned about the security of IoT devices as vulnerable devices can provide a route for hostile actors to attack the IT systems used by businesses. As part of the government's work to address this issue and improve cyber resilience across the UK economy, the government commissioned NCC Group to conduct a vulnerability assessment of some commonly-used enterprise connected devices.

#INFOSEC2025: RANSOMWARE ENTERS 'POST-TRUST ECOSYSTEM,' NCA CYBER EXPERT SAYS

Infosecurity Magazine - The ransomware landscape has entered a "post-trust ecosystem," where fragmented and increasingly mistrustful cybercrime groups operate in a climate of heightened law enforcement scrutiny, according to William Lyne of the UK's National Crime Agency (NCA). The result is a more unpredictable and potentially more perilous threat environment for organizations worldwide. In recent years, a series of high-profile law enforcement takedowns has disrupted some of the most notorious ransomware groups. Now the dust is settling and a cybercrime landscape that's more splintered than ever is emerging.

GROWING CYBER TALENT THROUGH PUBLIC–PRIVATE PARTNERSHIPS

WEF - Public–private partnerships (PPPs) offer a promising approach to cybersecurity workforce development by leveraging the strengths of both the public and private sectors to support skills development, career growth and the creation of sustainable talent pipelines. The Growing Cyber Talent Through Public–Private Partnerships white paper aims to highlight the benefits of PPPs to both sectors, including financial sustainability, market access and infrastructure for cybersecurity education.

POWERING CYBER RESILIENCE IN THE ENERGY SECTOR

WEF - Technology changes are rapidly driving energy-sector growth and changing how energy is produced, moved and stored as demand increases and companies pursue hybridization, asset diversification and partnerships. At the same time, escalating cybersecurity threats against energy infrastructure are making cyber resilience a necessary component of continued growth. Addressing these changing needs requires greater collaboration across the energy sector to build resilience into energy systems.