DIGI AMERICAS ALLIANCE MEMBERS

COMMISSION RECEIVES DETAILS ON MITIC'S CYBERSECURITY PLAN - PARAGUAY

Senate of Paraguay - During the meeting, Minister Gustavo Villate presented the National Cybersecurity Strategy 2025–2028, recently formalized through Executive Decree No. 3900. He noted that this instrument marks a momentous step toward consolidating a more secure and inclusive digital ecosystem in the country. "The document consolidates the update process initiated in March 2024, based on the progress of the 2017 National Cybersecurity Plan. It emerges as a response to the need to adapt to a constantly evolving digital environment," the minister explained.

THE PARAGUAYAN DIGITAL PATH FOCUSES ON CENTRALIZATION, 5G, AND CYBERSECURITY

abc Paraguay - As the global technology market evolves, Paraguay is accelerating its digital agenda with investments in connectivity, cybersecurity, and data centers. With key public initiatives and support from the private sector, the country seeks to position itself as a competitive player in the regional digital economy.

TWO KEY DAYS FOR NATIONAL CYBERSECURITY AND THE IMPLEMENTATION OF THE NEW LAW - CHILE

trendtic.cl - With an important announcement from the National Cybersecurity Agency (ANCI) regarding the start of the qualification process for Operators of Vital Importance (OIV), the two-day event "Patagonia Ciber 2025" concluded this Friday in Puerto Varas. This first major national cybersecurity gathering, organized by Fundación País Digital and ANCI, brought together more than 500 people per event, including prominent economic and business leaders and authorities, to address the challenges and advances in the field under the new Chilean legal framework.

ARMY CONSOLIDATES CYBERSECURITY WITH DATA CENTER IN SÃO PAULO - BRAZIL

LRCA - The 3rd Area Telematics Center (3rd CTA) opened a data center on May 29th in the capital of São Paulo. Named Data Center Marechal Rondon, the data processing center reinforces the capabilities of the Coronel Ricardo Franco Data Center, located in Brasília (DF), and consolidates the cybersecurity of the Land Force. The Data Center Marechal Rondon will be a pillar in supporting strategic decision-making, providing real-time data, advanced analysis and reliable information support to the High Command of the Brazilian Army. Its infrastructure allows for the secure and rapid exchange of information between different operational and institutional levels.

BRAZIL GAINS FIRST INTEGRATED CYBER INTELLIGENCE CENTER

Canção Nova - The country's first Integrated Cyber Intelligence Center was opened in the Administrative City in Minas Gerais. The intention is to monitor threats made in the digital environment and help prevent attacks on educational institutions.

GOVERNMENT SUSPENDS SEVEN BETTING SITES DUE TO DIGITAL SECURITY FAILURE; SEE LIST - BRAZIL

g1 - The Finance Ministry's Prize and Betting Department (SPA/MF) suspended seven fixed-odds sports betting operators and all their respective websites this Friday (30). The companies failed to comply with the regulation's requirements by failing to submit mandatory system security assessment reports. With the decision, the websites are prohibited from offering bets, accepting deposits or registering new users in Brazil until they submit the required documents. If they continue to operate, they will be fined R$40,000 per day.

CYBERATTACKS AGAINST CRITICAL INFRASTRUCTURE IN MEXICO ARE ON THE RISE

almomento - In Mexico, critical infrastructure is increasingly exposed to cyberattacks that could cripple essential services. Cybersecurity experts warn that a lack of software updates, regulatory gaps, and a shortage of specialists have made the country vulnerable to malicious actors. Over the past year, there has been an increase in attempted breaches into strategic networks such as electrical systems, water treatment plants, and hospital platforms. These attacks seek to disrupt operations, manipulate data, or cause physical damage by exploiting gaps in digital security.

ATTENTION: CYBERATTACKS WARNED ABOUT THE ELECTION OF THE JUDICIARY IN MEXICO

dplnews - For the first time in Mexico, there will be an election for the Judiciary (judges and magistrates) on June 1st, and cybersecurity specialists have already warned of possible attacks, both against the institutions involved in the process and against citizens themselves. According to the cybersecurity firm Netscout Systems, there has been a 218 percent increase in Distributed Denial of Service (DDoS) attacks against critical infrastructure in the country, coinciding with the electoral situation.

CYBERSECURITY REGULATION IS A PENDING TASK IN MEXICO: AMCS

El Economista - Despite the growing volume of personal information handled by public institutions in Mexico and the emergence of new legislative initiatives on digital matters, the country still lacks a comprehensive regulatory framework for cybersecurity. This was stated by Ernesto Ibarra, coordinator of the Mexico Cybersecurity Alliance (AMCS) and president of the Mexican Association of Cybersecurity and Digital Law (Amcid), in an interview with El Economista.

FINANCIAL CYBERSECURITY IN THE BANKING SECTOR - MEXICO

idc - Digital security is an increasingly relevant issue, and when it comes to money, it's even more important. Therefore, the Mexican government and banking sector are investing in financial cybersecurity. In this regard, the outgoing president of the Mexican Banking Association (ABM), Julio Carranza Bolívar, mentioned at the 88th Banking Convention held in Nayarit that nearly 21 billion transactions are currently processed annually through the banking system, or "2.4 million transactions per hour, 675 per second."

CYBERSECURITY MUST CONSIDER THE PROTECTION OF HUMAN RIGHTS - MEXICO

Gaceta UNAM - With the arrival of neurotechnologies that promise to help combat depression or implant chips in the brain to connect them to computers, it is important to be aware of the need to protect our biometric data (which includes brain waves) to prevent misuse. This was recommended by Anahiby Becerril Gil, an academic from the General Directorate of Computing and Information and Communication Technologies (DGTIC) at UNAM. She specified that the "handing over" of this type of information—our face, voice, iris, and fingerprint—has become increasingly normalized in society when using so-called smart devices (cell phones, watches, tablets, hearing aids), without questioning who it is being sent to, what it is being used for, how long it will be retained, or for what purposes.

WHAT CHALLENGES DO GOVERNMENTS FACE IN THE FACE OF DIGITALIZATION AND DATA PROTECTION? EXPERTS POINT OUT

Infobae - Governments and businesses face the challenge of maintaining control over their data and technologies in a globalized environment. Digital sovereignty involves developing local capabilities in infrastructure, software, and regulation to protect technological autonomy and comply with international standards. Governments seek to modernize their services through digitalization, but face obstacles such as resistance to change, budgetary constraints, and the need to ensure digital inclusion.

WHY CYBER RESILIENCE SHOULD BE A TOP PRIORITY FOR FREIGHT FORWARDERS

WEF - Freight forwarders are accelerating digitalization to boost efficiency, but this also increases vulnerability to cyber threats. Ransomware attacks show how even short disruptions can ripple through supply chains, especially impacting small and medium-sized forwarders. FIATA is leading efforts to strengthen cyber resilience through practical guidance, training, and tools for the global freight forwarding community.

CYBER ATTACKS AND RANSOMWARE RISE GLOBALLY IN EARLY 2025

digwatch - Cyber attacks have surged by 47% globally in the first quarter of 2025, with organisations facing an average of 1,925 attacks each week. Ransomware activity alone has soared by 126% compared to last year. Attackers are no longer just encrypting files but now also threaten to leak sensitive data unless paid — a tactic known as dual extortion. Instead of operating as large, centralised gangs, modern ransomware groups are smaller and more agile, often coordinating through dark web forums, making them harder to trace.