DIGI AMERICAS ALLIANCE MEMBERS

GUATEMALA PRESENTS INITIATIVE IN RESPONSE TO THE RISE IN CYBERATTACKS

Congress.gob.gt - In response to the cyberattacks against various state entities in recent weeks, members of the Viva bloc, including Representative Gerson Barragán, Third Secretary of the Board of Directors; Edin de Jesús and Obbed Castañasa, the bloc's leader and deputy leader respectively, presented a bill on Tuesday seeking to create a national cybersecurity system. At a press conference, the bloc leader explained that the proposal contains 76 articles aimed at establishing a comprehensive legal framework for the prevention, management, and response to cyber risks that affect public services and citizens' personal data.

CYBERSECURITY LAW PROMOTED IN HONDURAS; WHAT IS IT ABOUT?

Tiempo - Liberal Party Representative José Rolando Sabillón announced his intention to promote a Cybersecurity Law for inclusion in the package of reforms to the Penal Code that is about to be debated in the National Congress. Sabillón pointed out that the country faces a significant lag in this area and lacks foundational legislation to structure a national cybersecurity system. He explained that Honduras currently lacks comprehensive regulations to serve as a basis for addressing cybercrime. “We are in our infancy when it comes to cybersecurity. We don't have a law that serves as a foundation, as a solid basis for confronting these crimes,” the congressman stated.

DECEA, FROM THE BRAZILIAN AIR FORCE, DISCUSSES SATELLITES AND CYBER DEFENSE IN AVIATION AND INDICATES MEASURES FOR AIR TRAFFIC SAFETY

Defesa TV - On May 4th, the Department of Airspace Control, a branch of the Brazilian Air Force, brought together experts from SISCEAB for a strategic discussion on the use of satellites and cyber defense in aviation. The agenda highlighted the evolution of aeronautical telecommunications, with the expansion of SATCOM and radio frequency communications, as well as the D2D concept, increasing the resilience and continuity of services.

NEARLY 15 MILLION ECUADORIAN IDENTITY RECORDS HAVE SURFACED ON CLANDESTINE NETWORKS AND FORUMS: AUTHORITIES ARE INVESTIGATING A NEW MASSIVE DATA BREACH

Infobae - A new cybersecurity alert shook Ecuador this week after specialized platforms detected the alleged leak of nearly 15 million Ecuadorian citizens' identity records on clandestine forums and social media. The exposed information reportedly includes full names, national identity card numbers, passport-style photos, signatures, and biometric data associated with the national identification system.

CYBER POLICE STRENGTHEN ACTIONS AGAINST ELECTRONIC FRAUD IN THE STATE OF MEXICO: THESE ARE THE RECOMMENDATIONS - MEXICO

Infobae - The Cyber Police of the State of Mexico have strengthened measures to combat electronic fraud in response to an increase in reports related to online purchases and sales. In a statement released through its official channels, the State Security Secretariat (SSEM) warned that the widespread use of digital platforms, social media, and messaging applications has facilitated scams that affect the population of the State of Mexico. The agency recommended strengthening prevention habits and reporting incidents to reduce risks in electronic transactions.

CYBERSECURITY: THE NEW DEFENSE IN DIGITAL TIMES - MEXICO

Cronica - In an increasingly interconnected world, cyberattacks have become one of the main threats to businesses, public institutions, and organizations of all sizes. Data theft, ransomware, and online fraud are everyday risks that have triggered a growing demand for specialists capable of anticipating, detecting, and neutralizing threats. In response, the Cisco Networking and Cybersecurity Lab at the Autonomous University of Guadalajara (UAG) is establishing itself as a strategic space for training "digital guardians." Supported by the global Cisco Networking Academy program, this center allows students to acquire skills in network configuration, vulnerability analysis, incident management, and secure architecture design, as well as prepare for international certifications that strengthen their professional profile.

GOODBYE TO TRADITIONAL PASSWORDS: THIS IS HOW THE NEW ERA OF DIGITAL CYBERSECURITY IS ADVANCING

Infobae - The traditional password model is becoming obsolete. In a system where more than 90% of security incidents originate from weak, stolen, or reused credentials, experts and organizations warn that the industry is moving toward more secure authentication systems. This trend is gaining momentum on World Password Day, driven by the rise in attacks such as personalized phishing and credential stuffing, which exploit vulnerabilities in the use of traditional passwords.

DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 7, 2026

CISA TELLS CRITICAL ORGANIZATIONS TO PREPARE FOR CYBER OUTAGES - USA

Federal News Network - CISA's new "CI Fortify" initiative notably pushes water utilities, the transportation sector and other critical infrastructure organizations to plan for a "geopolitical crisis" involving cyber attacks that could sever their connections to internet, telecommunications and other technology services. CISA's guidance features two primary emergency planning objectives: "isolation" and "recovery" to mitigate threats. The former involves "proactively disconnecting from third-party and business networks" to safeguard operational technology, such as industrial control systems, from cyber attack during a crisis. CISA says organizations should be prepared to sustain "essential operations" rather than completely shutting down.

NIST WILL TEST THREE MAJOR TECH FIRMS' FRONTIER AI MODELS FOR CYBERSECURITY RISKS - USA

Cybersecurity Dive - The U.S. government's AI security center will evaluate frontier models from Google, Microsoft and xAI before their release to determine whether the models' advanced capabilities pose cybersecurity risks. The newly announced plan for the National Institute of Standards and Technology's (NIST) Center for AI Standards and Innovation (CAISI) to conduct "pre-deployment evaluations" represents the U.S. government's most significant attempt yet to get ahead of security threats from powerful AI systems. "Independent, rigorous measurement science is essential to understanding frontier AI and its national security implications," CAISI Director Chris Fall said in a statement. "These expanded industry collaborations help us scale our work in the public interest at a critical moment."

EMPOWERING DEFENDERS: AI FOR CYBERSECURITY

WEF - AI is transforming cybersecurity, but realizing its full value requires strategic deployment, robust governance and balanced human oversight. This white paper, Empowering Defenders: AI for Cybersecurity, offers practical guidance for organizations seeking to harness AI in their cybersecurity efforts. To support effective implementation, the paper outlines the critical questions executives and chief information security officers must address and provides an early perspective on the opportunities and challenges posed by agentic AI. It suggests that executive and cyber leaders embarking on the AI adoption journey for cyber defence should: align the adoption of AI in cybersecurity with enterprise strategic priorities; establish organizational readiness across processes, data, infrastructure, skills and governance before deploying AI in cybersecurity; validate AI solutions through structured pilots prior to full deployment; and scale and monitor the performance of AI in cybersecurity and optimize as needed.

TARGET-RICH, CYBER-POOR: HOW TO STRENGTHEN CYBERSECURITY AND BUILD RESILIENCE IN VULNERABLE SECTORS

WEF - In June 2025, cyberattacks on two hospitals in north Delhi severely disrupted access to digital patient records, forcing staff to activate manual systems for patient care to maintain services during the incident. In September that same year, a ransomware attack on UK-based early childhood education provider Kido International exposed sensitive data of around 8,000 children and staff, including names and photographs. Both breaches triggered national cybersecurity warnings and led to the arrests of the perpetrators, underscoring the real-world risks cyberattacks pose to vulnerable communities. The World Economic Forum's Global Cybersecurity Outlook 2025 highlighted that the growing complexity of cyberspace is exacerbating cyber inequity, widening the gap between sectors.