DIGI AMERICAS ALLIANCE MEMBERS

NATIONAL CYBERSECURITY STRATEGY - BRAZIL

Institutional Security Office - The new National Cybersecurity Strategy (E-Ciber) was established by Decree 12,753 of August 4, 2025. This is the second version of the Brazilian document on this topic (the first was issued in 2020), bringing a new level of maturity and governance to the country's cybersecurity. In context, E-Ciber arises from the National Cybersecurity Policy and was proposed by the National Cybersecurity Committee, which brings together 25 institutions, including federal government agencies, representatives of civil society organizations, scientific institutions, and the business sector, all related to cybersecurity.

GOVERNMENT ESTABLISHES THE THIRD GENERATION OF THE NATIONAL INFORMATION SECURITY POLICY - BRAZIL

EBC - President Lula signed Decree No. 12,572/2025, which establishes the National Information Security Policy (PNSI) in the federal public administration. Published this Tuesday (August 5th) in the Official Gazette of the Union (DOU), the measure consolidates a new framework for data and systems protection, with guidelines, objectives, and a governance structure to ensure the availability, integrity, confidentiality, and authenticity of the country's information.

CYBER DEFENSE OPERATIONS CENTER OPENS IN BRASILIA, BRAZIL

EBC - Aiming to strengthen national capabilities in the cyber domain, the Cyber Defense Operations Center (CDCiber) was inaugurated this Monday (August 4th). With a total area of over 2,750 square meters, the new facility houses 194 integrated workstations, with environments adaptable to the nature of operations. The space features a Tier II Data Center, meeting international standards with availability exceeding 99.75%, as well as redundant power and cooling systems that ensure the unit's uninterrupted operation.

GUATEMALA WILL RECEIVE A US$300 MILLION INVESTMENT TO BUILD A STATE-OF-THE-ART DATA CENTER

Prensa Libre - The new data center could have Amazon and Google as clients, will connect the country with India, Dubai, and the US, and will generate some 700 jobs in areas such as cybersecurity and artificial intelligence. Guatemala will receive the region's first fourth-generation data center. The initial investment will be US$300 million, and according to Janio Rosales, CEO of Innovaton Strategies and partner and member of the Board of Directors of the consortium with Aurum Equity Partners and Bold Capital Group, this is one of the largest technology investments to be made in Central America.

THE NATIONAL ASSEMBLY PLENARY SESSION DEBATES REFORMS TO THE DIGITAL TRANSFORMATION LAW TO STRENGTHEN CYBERSECURITY IN ECUADOR

kch - Based on the report prepared by the Commission on Sovereignty, Integration, and Comprehensive Security, the Plenary Session of the National Assembly analyzed in its first debate the draft Organic Law for the Strengthening of Cybersecurity, an amendment to the Organic Law on Digital and Audiovisual Transformation. "Ecuador is the third country in the region with the highest number of cyberattacks, which is why it records annual losses of between $200 and $600 million," explained the report's rapporteur, Inés Alarcón, when explaining the need for a regulatory framework to prevent this phenomenon through a solid national cybersecurity policy.

ANCI PUBLISHES ACTION PLAN FOR THE NATIONAL CYBERSECURITY POLICY 2023–2028 IN THE OFFICIAL GAZETTE - CHILE

trendTIC - Santiago, August 6, 2025. The Official Gazette published Exempt Resolution No. 28, issued by the National Cybersecurity Agency (ANCI), which formalizes the implementation of the Action Plan of the National Cybersecurity Policy 2023-2028, following its unanimous approval by the Interministerial Cybersecurity Committee on March 27, 2025. The resolution is based on the current regulatory structure, which includes Law No. 21,663 — which created the National Cybersecurity Agency as a decentralized public service— and Supreme Decree No. 164 of 2023, which approved the national policy in this area.

THE PROCESSING OF THE AI BILL IN CHILE CONTINUES

iapp - The Bill regulating Artificial Intelligence Systems (Bulletin No. 16,821–19), which is currently in its first constitutional process after its Financial Report was rejected by the Finance Committee in early July 2025, does not restrict its continued legislative process. It is important to remember that this bill, in its latest submitted version, aims to regulate and promote the creation, development, innovation, and implementation of AI systems at the service of people, respectful of democratic principles and the rule of law (Article 1). It applies to those providers that introduce AI systems to the market or put into service, AI system implementers, as authorized representatives of AI system providers, when said importers, distributors, or authorized representatives are located in Chile.

THE US DONATES TECHNOLOGICAL EQUIPMENT TO SUPPORT THE DIGITALIZATION OF THE DOMINICAN JUSTICE SYSTEM

acento - The Dominican judiciary received a technology donation from the U.S. Embassy's Office of International Narcotics and Law Enforcement Affairs (INL) to promote the digital transformation of the judicial system. The donation includes more than 100 workstations, scanners, microcomputers, backup systems, and firewalls to protect networks and devices.

UAQ AND UNAM PROMOTE THE CREATION OF A SPECIALIZED CENTER FOR CYBERSECURITY - MEXICO

lideres empresarial - To strengthen the digital infrastructure in Querétaro, the Autonomous University of Querétaro (UAQ) and the National School of Higher Studies Juriquilla Unit (ENES) of the National Autonomous University of Mexico (UNAM) formalized a collaboration agreement to create a Cybersecurity Operations Center (SOC) in the state. This document establishes the foundation for both institutions to work together in the consulting, training, and operational design of the center, which will aim to address the cybersecurity challenges facing universities in an increasingly interconnected global environment.

ADVANCED ORGANIZED CRIME EXPOSES CRITICAL CYBER-GAPS IN MEXICO

Mexico Business News - Mexico faces a growing and dangerous cybersecurity threat as sophisticated criminal groups adopt advanced technologies to diversify their illicit operations. The situation has positioned the country as a primary target for cyberattacks in Latin America, with a volume of incidents that reveals a concerning asymmetry between attacker capabilities and the defense strategies of the public and private sectors. “Today, the fight against cybercrime gang leaders requires a strategy based on structured intelligence rather than mere declarations of goodwill. However, the institutional response has been weak and fragmented,” says Victor Ruiz, Founder, Silikn.

U.S. SENATE CONFIRMS SEAN CAIRNCROSS AS THE NATIONAL CYBER DIRECTOR

White House - Today, the United States Senate confirmed Sean Cairncross as the National Cyber Director. He will serve as President Trump’s principal advisor on national cybersecurity policy and strategy. “I want to thank President Trump for this opportunity. It is an incredible honor to serve our country and this President as the National Cyber Director,” said Mr. Cairncross. “As the cyber strategic environment continues to evolve, we must ensure our policy efforts and capabilities deliver results for our national security and the American people.

GOOGLE WARNS: SCATTERED SPIDER TARGETS U.S. CRITICAL INFRASTRUCTURE WITH VMWARE-BASED CYBER ATTACKS

CPO Magazine - Google Threat Intelligence Group (GTIG) warns about highly sophisticated and aggressive cyber attacks by the Scattered Spider threat actors on critical infrastructure. According to GTIG, the threat group leverages social engineering tactics to breach domain user accounts and gain administrative privileges before pivoting to virtualized environments, such as VMware.

THE GROWING IMPACT OF AI AND QUANTUM ON CYBERSECURITY

Cybercrime Magazine - The amalgamation of artificial intelligence (AI) with quantum computing will transform existing computational paradigms, heralding a promising future, but with risks, writes Chuck Brooks in a Forbes article. While AI and machine learning (ML) are crucial tools for cyber defense, they may also provide asymmetrical tools for adversarial hackers. Their favored techniques include automated phishing schemes that replicate human actions, with malware that autonomously alters itself to mislead or compromise cybersecurity frameworks and applications.