DIGI AMERICAS ALLIANCE MEMBERS

Apple aws Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks
Google kriptos LUMU netskope paloalto NETWORKS Resecurity
Schneider Electric SISAP Sistemas Aplicativos Strike Telefónica tenable Trellix TREND MICRO

NATIONAL GUARD RECEIVES CERT-MX DECLARATION OF COMPLIANCE UNDER THE SIM3 CSIRTAMERICAS BASELINE MODEL - MEXICO

Indigo Report - The National Guard (GN) received today the Declaration of Compliance of the "CERT-MX" under the "SIM3 CSIRTAméricas Baseline" model, granted by the Organization of American States (OAS) through its "CSIRTAméricas" program, which is a fact that consolidates Mexico's commitment to national and regional cybersecurity.

THE YUCATÁN CYBERSECURITY FORUM 2025 SEEKS TO CONSOLIDATE THE STATE AS A DIGITAL BENCHMARK IN MEXICO

El Sol de Mexico - In an increasingly interconnected world, cybersecurity has become a priority issue for both businesses and citizens. From corporations that must secure their processes and technologies to ordinary users who face risks such as extortion, electronic fraud, and identity theft, the digital threat is constant and growing. Mexico now ranks second in Latin America in the number of cyberattacks, with more than 80 billion attempts blocked in 2024 alone, according to figures from international digital security firms.

SENATORS ADVANCE IN CREATING A REGULATORY FRAMEWORK TO REGULATE ARTIFICIAL INTELLIGENCE IN MEXICO

DPL News - The president of the Commission for Analysis, Monitoring, and Evaluation of the Application and Development of Artificial Intelligence in Mexico, Rolando Rodrigo Zapata Bello, reported that a proposal for a new law on this matter has been provided to the members of this legislative body. During the regular meeting this Tuesday, the senator said that the goal is to advance the construction of a solid regulatory framework and explained to the senators that on September 19, they were sent the proposal with the chapters that could be included in the General Law to Regulate and Promote the Use of Artificial Intelligence in Mexico.

CYBERATTACKS AND DATA PROTECTION: CHALLENGES FACING PANAMANIAN BANKING

La Estrella - This sector requires key and effective communication to all clients and users to work together to protect the system throughout Panama and Latin America. Ernesto Boy, president of the board of directors of the Panamanian Banking Association (ABP), warned of the growing threat of cyberattacks and the need for ongoing preparedness in the sector. His remarks were made during a regional conference on risk management that brought together more than 370 participants from Latin America in Panama City.

ANCI AND THE CHILEAN SENATE SIGN A COLLABORATION AGREEMENT TO STRENGTHEN CYBERSECURITY

Segurilatam - The Senate of the Republic of Chile and the National Cybersecurity Agency (ANCI) signed a cooperation agreement on September 29 in Santiago, a key element of the country's digital transformation. This agreement is the first signed by the Agency with an autonomous constitutional body. Specifically, it establishes a cooperation mechanism that will allow collaborative work on cybersecurity matters between both institutions. The objective is to guarantee and strengthen cybersecurity, as well as to prevent and manage potential cybersecurity incidents in a timely and appropriate manner.

DATA LEAK HIGHLIGHTS FRAGILITY OF HEALTH SECTOR, ANALYSIS FINDS - BRAZIL

Security Leaders - Hospitals and clinics in Brazil face an increasingly challenging scenario due to the escalation of cyberattacks. According to an intelligence report from ISH Tecnologia, more than 11,000 security incidents were recorded in the first half of 2025 alone, and almost all had a direct impact on healthcare institutions. Although they represent about 6.7% of all ransomware attacks in the country, incidents in the sector generate disproportionate consequences, compromising medical care, leaking sensitive patient data, and causing millions in losses.

SENATIC AND ELEMPLEO.COM JOIN FORCES TO TRAIN THE PROFESSIONALS OF THE FUTURE - COLOMBIA

Mintic.gov.co - United for the country's academic and professional development, the Ministry of Information and Communications Technology (ICT), the International Labor Organization (ILO), the National Learning Service (Sena), and elempleo.com signed a strategic alliance to bring new digital training opportunities to millions of Colombians. The agreement seeks to expand the impact of the SenaTIC program by connecting the free digital skills training it promotes through certified online short courses with the platform's effective employability pathways. As a result of this alliance, elempleo.com users will be able to take courses from technology giants such as Google, Microsoft, IBM, Meta, and Amazon on the Coursera platform.

CYBERTHREAT SHARING LAW EXPIRES AS GOVERNMENT SHUTS DOWN - USA

The Hill - A law allowing private companies to share information about cybersecurity threats with the government expired Wednesday after Congress failed to reauthorize the legislation amid a wider shutdown fight. The Cybersecurity and Information Sharing Act (CISA) of 2015, which initially appeared poised to be extended as part of a temporary stopgap measure, lapsed as lawmakers failed to avert a shutdown — a pause that lawmakers and experts warn could restrict a key pipeline of threat intelligence.

CISA EMPHASIZES NEED FOR OPERATIONAL TECHNOLOGY VISIBILITY IN WATER, ENERGY SECTORS - USA

Inside Cybersecurity - Federal officials from Cybersecurity and Infrastructure Security Agency and the Energy Department highlighted the need for utilities to maintain visibility into their operation technology systems, at a virtual event highlighting recent OT asset inventory guidance developed through the Joint Cyber Defense Collaborative. “This product is the result of JCDC ongoing partnership and engagement with operational technology and industrial control systems stakeholders,” JCDC associate director Clayton Romans said on a Sept. 30 webinar hosted by CISA.

CISA ADVANCES NATIONAL CYBER RESILIENCE WITH DIRECT SUPPORT TO STRENGTHEN SLTT PARTNERS - USA

Industrial Cyber - The U.S. Cybersecurity and Infrastructure Security Agency (CISA) announced it is moving to a new model designed to better equip state, local, tribal, and territorial (SLTT) governments in defending against cyber threats. The shift provides SLTT partners with grant funding, no-cost tools, and direct cybersecurity expertise to build resilience and strengthen local leadership in national security.

CISA, FBI, UK NCSC URGE ORGANIZATIONS TO ALIGN OT SECURITY PRACTICES WITH IEC 62443, ISO/IEC 27001 STANDARDS

Industrial Cyber - The U.S. Cybersecurity and Infrastructure Security Agency (CISA), working with the Federal Bureau of Investigation, the U.K.’s National Cyber Security Centre (NCSC), and other international partners, has released joint cybersecurity guidance for OT (operational technology) environments. The document provides a definitive OT record that helps organizations conduct more comprehensive risk assessments, prioritize critical and exposed systems, and implement stronger security controls.

LIMITING THE BLAST RADIUS OF MODERN CYBER ATTACKS

Forbes - The toughest part of most cyberattacks isn’t the break-in. It’s what happens after. Once an attacker is inside, they move sideways—testing connections, escalating privileges and spreading until a small crack turns into a gaping wound. I’ve been covering this space for years, and what strikes me is how often we keep relearning the same lesson: prevention is never perfect, and it’s the spread that really does the damage.