DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 17, 2025

DIGI AMERICAS ALLIANCE MEMBERS

CHILE PUBLISHES THE REGULATIONS FOR THE OPERATION OF THE STATE SECURE CONNECTIVITY NETWORK

SeguriLatam - The Official Gazette of the Republic of Chile has published the regulations establishing the operation of the State Secure Connectivity Network (RCSE), a critical infrastructure that digitally connects public agencies and is now formalized as part of the implementation of the Cybersecurity Framework Law. Thus, this network, administered by the National Cybersecurity Agency (ANCI), is the legal successor to the former State Connectivity Network created in 1999. Its modernization and regulation represent a decisive step toward strengthening the digital resilience of the Chilean State.

THE ARMY PROJECTS DIRECTORATE AND CIBERLAB UC HELD A WORKING MEETING - CHILE

Chilean Army - As part of the multiple academic and research initiatives uniting the Chilean Army and the Pontifical Catholic University, the Projects Directorate, together with the Army Intelligence Brigade, attended the UC Cyberlab, which was born from the alliance with the university's Innovation Center. The purpose of the working meeting was to provide feedback on the progress of the joint cyber defense projects being implemented under the dual innovation modality between both institutions, from 2024 to the present.

CONGRESSMEN WILLING TO SUPPORT CYBERSECURITY BILL - MEXICO

La Prensa - The role of the legislators of the Mexico City Congress will be essential for the approval of the Cybersecurity Law initiative aimed at the city's obligated subjects as soon as possible, acknowledged the president commissioner of the Institute of Transparency, Access to Public Information, Protection of Personal Data and Accountability of Mexico City (INFO), Laura Lizette Enríquez Rodríguez, when explaining that this proposal aims to consolidate a robust regulatory framework for the protection of the references of all citizens, who are increasingly exposed to risks derived from digitalization.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 17, 2025

WAR GAMES GAIN PROMINENCE IN NATIONAL STRATEGIC PREPARATION - BRAZIL

Defesa em foco - From an oil spill simulation to defense strategies for the Rio Olympics, the War Games have become a key part of Brazil's security and sovereignty planning. At the Naval War College (EGN), where the country's main center operates, civilian and military leaders test solutions for threats ranging from cyber warfare to interagency coordination, natural disasters and border operations.

FIVE CYBERSECURITY THREATS IN 2025: WHAT TO EXPECT? - BRAZIL

Privacy Tech - As technology advances, so do cybersecurity threats, especially in an increasingly connected world. By 2025, experts have identified five major threats that could affect both individuals and organizations. These threats not only reflect the increasing sophistication of cybercriminals, but also the urgent need for greater awareness of digital security.

REQUEST FOR REPORTS FROM THE MINISTRY OF INFORMATION AND COMMUNICATIONS (MITIC) ON CYBERSECURITY AND DATA BREACHES APPROVED - PARAGUAY

Diputados.gov.py - In its last regular session, the Chamber of Deputies approved, on the spot, a draft resolution "Requesting reports from the Executive Branch - Ministry of Information and Communication Technologies (MITIC)" on the status of cybersecurity within government structures. The initiative was sponsored by Representative Raúl Benítez (Independent-Central), who raises the need to clarify the measures adopted by MITIC in relation to the National Cybersecurity Plan.

THREE YEARS AFTER THE HACKING OF THE MINISTRY OF FINANCE: HOW ARE COSTA RICA'S PUBLIC INSTITUTIONS DOING IN CYBERSECURITY? - COSTA RICA

El Financiero - After Easter 2022, the Ministry of Finance's systems were blocked by the Conti cybercriminal group, but other entities were attacked at that time and later. Has cybersecurity improved in public institutions?

PANAMA: WILL HOST IMPORTANT CYBERSECURITY EVENT

Critica - From May 21 to 23, 2025, Panama will host the 5th STIC Congress RootedCON Panama Chapter, a leading international event in the field of cybersecurity, which will take place at the Panama Convention Center (Amador), in Panama City, for the second consecutive year in the country.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 17, 2025

COLOMBIA STRENGTHENS ELECTORAL CYBERSECURITY WITH FACIAL RECOGNITION AND EARLY WARNINGS

Hoy Diario del Magdalena - With the goal of ensuring more secure electoral processes, the National Civil Registry, in conjunction with the National Police, announced a technological security system that integrates facial biometric validation with the criminal record database.
This measure will seek to anticipate risks and strengthen the cybersecurity of the Colombian electoral system ahead of the 2025 and 2026 elections.

CHINA ADMITS BEHIND CLOSED DOORS IT WAS INVOLVED IN VOLT TYPHOON ATTACKS

Yahoo News - Amid a serious escalation of hostilities between the two nations, senior Chinese officials have apparently acknowledged behind closed doors that Beijing was involved in a series of cyberattacks on US critical infrastructure. These attacks saw Chinese Volt Typhoon hackers infiltrate US critical infrastructure systems for years, including compromising energy, communications, transportation, and water industries.

NIST UPDATES PRIVACY FRAMEWORK, TYING IT TO RECENT CYBERSECURITY GUIDELINES

NIST - How can society benefit from the use of personal data while also protecting individual privacy? Five years after debuting guidelines that can help organizations balance these goals, the National Institute of Standards and Technology (NIST) has drafted a new version of the NIST Privacy Framework intended to address current privacy risk management needs, maintain alignment with NIST's recently updated Cybersecurity Framework, and improve usability. The draft release, NIST Privacy Framework 1.1 Initial Public Draft, is broadly intended to help organizations manage the privacy risks that arise from personal data flowing through complex information technology systems.

CYBERSECURITY IN THE AI ERA: EVOLVE FASTER THAN THE THREATS OR GET LEFT BEHIND

The Hacker News - AI is changing cybersecurity faster than many defenders realize. Attackers are already using AI to automate reconnaissance, generate sophisticated phishing lures, and exploit vulnerabilities before security teams can react. Meanwhile, defenders are overwhelmed by massive amounts of data and alerts, struggling to process information quickly enough to identify real threats. AI offers a way to level the playing field, but only if security professionals learn to apply it effectively.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 17, 2025

CYBERSECURITY RISKS OF ENCRYPTION BACKDOORS: WHAT BUSINESS LEADERS SHOULD KNOW

Forbes - The Washington Post reported in February that the U.K. government issued a "secret order" that "demanded that Apple create a back door allowing them to retrieve all the content any Apple user worldwide has uploaded to the cloud." While the immediate order is centered on Apple's cloud data, the U.K.'s order for blanket access to encrypted material raises broader questions about its applicability to other companies and its potential to undermine end-to-end encryption, a critical tool businesses and consumers broadly rely upon today to keep their devices, services and data safe.

OPTIMIZING CYBERCRIME DETECTION: A HYBRID DEEP LEARNING APPROACH FOR ENHANCED INTRUSION DETECTION SYSTEMS

With the rapid advancement of technology, servers have become increasingly vulnerable to cyber threats, posing significant risks to valuable assets such as cloud infrastructure, IoT devices, and mobile applications. As cyberattacks escalate across various industries, the role of intrusion detection systems (IDS) in maintaining cybersecurity has become more critical than ever. Traditional (IDS) face substantial challenges in analyzing large volumes of operational data, often relying on recorded attack instances and anomaly detection, which may not suffice in the face of evolving threats. To overcome these limitations, recent advancements have focused on leveraging machine learning and deep learning-based (IDS).