DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 9, 2025

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks Google LUMU METABASE Q netskope paloalto NETWORKS Resecurity Schneider Electric SISAP Telefónica tenable Trellix TREND MICRO

THE NATIONAL CYBERSECURITY AGENCY (ANCI) BEGINS OPERATIONS AND THE PRESIDENT APPOINTS DANIEL ÁLVAREZ AS ITS FIRST DIRECTOR - CHILE

Trendtic - In the process of implementing the Cybersecurity Framework Law 21,663, unanimously approved by Congress in December 2023, the National Cybersecurity Agency (ANCI) began operating on Thursday, January 2. The Framework Law, including the creation of the ANCI, is part of the government's prioritized security agenda. The new agency is part of the Government's Security Strategy, in the axes of strengthening institutions, combating organized crime - particularly to confront cybercrimes - and also in the search for State agreements on security matters. Among the powers of the ANCI is to supervise, regulate and sanction institutions that provide essential services, whether public or private, in the area of cybersecurity.

CYBERSECURITY FRAMEWORK LAW IN CHILE REQUIRES COMPANIES TO STRENGTHEN THEIR DIGITAL PROTECTION: GUIDE TO ALIGN WITH THE STANDARD

Emol - In response to the growing cyber threat landscape, Chile's recent Cybersecurity Framework Law requires organizations to take urgent measures to protect their critical systems and data. The law seeks not only to strengthen the country's digital security, but also to ensure that companies are prepared to respond effectively to potential attacks. Carolina Pizarro, Cybersecurity Associate Director at Accenture Chile, highlighted that the law requires companies to implement a series of key practices to strengthen their cybersecurity: “This includes not only the ability to respond quickly to incidents, but also to recover from them effectively, minimizing the impact on services and the population.”

FOREIGN AFFAIRS COMMITTEE EVALUATES NATIONAL CYBERSECURITY POLICY - BRAZIL

Senate - The evaluation report by Senator Esperidião Amin (PP-SC) highlights priorities for the sector that raises concerns due to increasing cyberattacks. Criticism of the creation of the National Cybersecurity Policy (decree no. 11,856/2023) by the government and the need for an agency are highlights in the rapporteur's text.

JOURNALISTS CONCERNED ABOUT NEW CYBERSECURITY LAW IN EL SALVADOR

CNN - El Salvador's Legislative Assembly has approved cybersecurity and personal data protection laws. According to some local organizations, and other international organizations such as Human Rights Watch, these norms could limit freedom of expression and access to information. For its part, the government rejects the criticism.

GOVERNMENTAL INFORMATION SECURITY SCHEME - ECUADOR

El Comercio - EGSI v3 in Ecuador strengthens public cybersecurity, protecting sensitive data through risk management, technical controls and regulatory compliance, guaranteeing digital security as a key right.

PROSECUTORS DISMANTLE CYBERCRIMINAL NETWORK THAT IMPERSONATED PUBLIC ENTITIES TO COMMIT FRAUD - COLOMBIA

Caracol - The Attorney General's Office, with the help of the National Police, managed to identify and capture three alleged members of a network of cybercriminals dedicated to impersonating public entities to distribute malicious emails. These messages contained software designed to extract personal and financial information from the devices of the victims, making it easier for them to commit thefts and other frauds.

THE CRISIS OF DIGITAL SILENCE IN ARGENTINA: THE DANGERS OF HIDING A CYBER ATTACK - ARGENTINA

Clarin - "Dani, how are you? I imagine you're more than aware of the Churruca issue and the ransomware cyberattack." A random Thursday became the day that the cybersecurity crisis I've been pointing out for years materialized in the voice of a friend: "My parents lost all their medical records and studies they had done. Especially my mother, who is undergoing active treatment... They lost all their appointments." A "madness," as he himself defined it, that exposes the true human dimension of our digital defenselessness.

SSPC WARNS OF INCREASING ONLINE FRAUD - MEXICO

La Jornada - The General Directorate of Service Management, Cybersecurity and Technological Development of the Secretariat of Security and Citizen Protection (SSPC) alerted citizens about the increase in online fraud and issued recommendations to avoid becoming victims of cybercriminals. It indicated that the ease of making purchases through various platforms, whether with a mobile device or a computer, has also increased the use of lures such as messages, calls and extraordinary offers by cybercriminals to steal user data and commit scams, so, it indicated, it is very important to take precautions.

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 9, 2025

CAVAPY REAFFIRMS ITS COMMITMENT TO THE MARKET BY GUARANTEEING INTERNATIONAL SECURITY AND ASSET PROTECTION - PARAGUAY

Marketdata - The Caja de Valores del Paraguay (Cavapy) has launched an ambitious cybersecurity program that not only seeks to align itself with the local requirements of the Superintendency of Securities and the Central Bank of Paraguay, but also to position itself as a regional benchmark, adopting international certifications such as ISO 27001 in its most recent version of 2022.

BIDEN ADMINISTRATION PROPOSES NEW CYBERSECURITY RULES TO LIMIT IMPACT OF HEALTHCARE DATA LEAKS

Reuters - Healthcare organizations may be required to bolster their cybersecurity, to better prevent sensitive information from being leaked by cyberattacks like the ones that hit Ascension and UnitedHealth (UNH.N), opens new tab, a senior White House official said Friday. Anne Neuberger, the U.S. deputy national security advisor for cyber and emerging technology, told reporters that proposed requirements are necessary in light of the massive number of Americans whose data has been affected by large breaches of healthcare information.

WHITE HOUSE LAUNCHES CYBERSECURITY LABEL PROGRAM FOR CONSUMERS

Cyberscoop - The White House announced Tuesday the official launch of the U.S. Cyber Trust Mark, a cybersecurity labeling initiative aimed at enhancing the security of internet-connected devices.
The initiative tackles rising consumer concerns about the security vulnerabilities of “smart” devices essential to modern homes. As households become more dependent on interconnected gadgets — with a 2023 Deloitte study revealing that the average U.S. household has 21 connected devices — the threat of cyberattacks becomes increasingly significant.

UN GENERAL ASSEMBLY ADOPTS MILESTONE CYBERCRIME TREATY

Global Issues - The General Assembly on Tuesday adopted the United Nations Convention against Cybercrime, a landmark global treaty aimed at strengthening international cooperation to combat cybercrime and protecting societies from digital threats. The agreement on the legally binding treaty marked the culmination of a five-year effort by UN Member States, with inputs from civil society, information security experts, academia and the private sector.

WHY COLLABORATION IS KEY TO DISRUPTING THE ECONOMICS OF CYBERCRIME

WEF - Businesses worldwide are embracing digital evolution. Yet cybersecurity implications inevitably emerge as technologies evolve and push us into a new era of connectivity. Adopting new technologies, devices and platforms increases potential points of compromise, widening an organization's attack surface. Having more digital systems to configure, integrate and manage leads to greater complexity and an increased likelihood of error.

DIGI AMERICAS LATAM CISO
INSIGHTS
JANUARY 9, 2025

THE TRUST IMPERATIVE: 5 LEVERS FOR SCALING AI RESPONSIBLY

WEF - At a recent conference, in a room with over 100 Fortune 500 founders, only two had mission-critical generative artificial intelligence (GenAI) use cases in production. The reason? Quality, accuracy and hallucinations are holding them back. This lack of trust in centring AI in their business was echoed in a recent Edelman study, which found that trust in AI companies in the United States has fallen from 50% to 35% over the last five years.

WHY SYSTEMIC INTERVENTION IS KEY TO MITIGATING CYBERCRIME

WEF - From the infrastructure that powers our villages and cities and the way we do business, to the ways we communicate with each other and entertain ourselves, we all rely on the internet. But the rise in internet use has been accompanied by an equivalent rise in attacks and cybercrime. Internet disruptions can be anything from annoying, to costly, to catastrophic. A massive data breach of background check company National Public Data in April 2024 leaked 2.9 billion US social security records, with class action lawsuits following.