



INSIGHTS

APRIL 3, 2025

DIGI AMERICAS ALLIANCE MEMBERS



NEW INTERMINISTERIAL CYBERSECURITY COMMITTEE APPROVES ACTION PLAN FOR THE NATIONAL CYBERSECURITY POLICY 2023-2028 - CHILE

trendTIC - Last Thursday, March 27, the first session of the new Interministerial Cybersecurity Committee was held. This committee was created by the Cybersecurity Framework Law to advise the President of the Republic on cybersecurity matters relevant to the country's operations, especially in the analysis and definition of the National Cybersecurity Policy and the measures, plans, and action programs that will be implemented for its execution.

OF NATIONAL INTEREST IS THE CREATION OF THE HIGH-LEVEL CYBERSECURITY COMMITTEE OF THE PERUVIAN STATE

Congressional News Center - The Science, Innovation, and Technology Committee unanimously approved the ruling on bills 8842/2024-CR and 9906/2024-CR, which propose declaring the creation of the Peruvian State High-Level Cybersecurity Committee of national interest and public necessity. This committee will regulate security in the use of technological tools and promote the creation of specialized agencies.

THE NATIONAL POLICE CONTINUES TO ADVANCE IN THE CREATION OF THE CENTRAL DIRECTORATE OF DIGITAL TRANSFORMATION - DOMINICAN REPUBLIC

National Police - The National Police held its second working meeting to discuss with internal and external stakeholders the proposal to create the Central Directorate of Digital Transformation, replacing the current Directorate of Information and Communication Technology. The meeting was held in the Strategic Thinking Room of the Central Directorate of Planning and Development (DIPLAN), in compliance with Resolution No. 342-2024 of the Ministry of Public Administration (MAP), which establishes the updating of the organizational structure models for the Digital Transformation and Cybersecurity units in Dominican State institutions.

WARNING ABOUT MASSIVE LEAK OF PARAGUAYAN DATA ON THE DARK WEB

abc.com.py - An alleged leak of personal data belonging to more than 7 million Paraguayans has raised alarm bells. The database, which allegedly included sensitive information such as names, addresses, and dates of birth, is reportedly being offered on the dark web for the equivalent of \$10,000. Cybersecurity experts warn of the seriousness of the incident and demand an urgent response from the government.

INA AND MINSAIT WILL PREPARE A CYBERSECURITY ASSESSMENT OF THE AUTO PARTS SECTOR - MEXICO

Mexico Industry - In a context where digital transformation is redefining the rules of the game for the automotive industry, cybersecurity is positioned as a key pillar for operational continuity, global competitiveness, and value chain protection. As part of this challenge, the National Auto Parts Industry (INA) has established a strategic alliance with Minsait, a leading company in digitalization and disruptive technologies within the Indra Group, with the goal of raising the level of digital maturity in terms of information security in the more than 700 manufacturing plants affiliated with the association.

INFO CDMX APPROVES CYBERSECURITY INITIATIVE - MEXICO

msn - The Mexico City Transparency Institute (Info CDMX) approved the initiative to issue the local Cybersecurity Law on Personal Data Protection and submit it to the Mexico City Congress. Commissioner President Laura Lizette Enríquez Rodríguez explained that this proposal grants INFO powers over cybersecurity related to personal data. It also establishes the obligation for public entities responsible for data processing to have a Cybersecurity Strategy, an Information Security Management System, and the duty to train public servants in this area.

MEXICO: DATA CENTER HUB

dplnews - Mexico has positioned itself as a strategic epicenter for the installation of data centers. With digital transformation, nearshoring, post-pandemic trends, and the rise of the cloud, the Internet of Things, and artificial intelligence, the demand for data centers has skyrocketed worldwide, and Mexico is emerging as a key hub in Latin America.

"EXPERTS IN THE DIGITAL ECONOMY" PROMOTE TECHNOLOGICAL TRANSFORMATION TO CLOSE OUT WOMEN'S MONTH 2025 - MEXICO

Ministry of Economy - As part of Women's Month, the Ministry of Economy, in collaboration with the Mexican Association of the Information Technology Industry (AMITI) and the National Chamber of the Electronics, Telecommunications, and Information Technology Industry (CANIETI), organized the event "Experts in the Digital Economy."

FEDERAL POLICE DISCUSS CHALLENGES AND COOPERATION IN COMBATING CYBERCRIME - BRAZIL

Security Report - The Federal Police held a seminar on the challenges of combating current cybercrimes and attacks. The discussion was aimed at Brazilian experts who have experience or are interested in learning more about how to deal with this type of crime and how to strengthen digital security. According to the General Coordination of Social Communication of the Federal Government, the PF Cybercrime Combat Directorate (DCIBER-PF) and representatives from the Czech Republic, Interpol, the Federal Public Prosecutor's Office and the Ministry of Foreign Affairs were present for this initiative.

DIGITAL TRANSFORMATION AND ITS IMPLICATIONS FOR BRAZIL'S ECONOMY

DOL - The Brazilian economy is changing rapidly due to technology. This change affects everything: commerce, industry, services, among other markets. And with this, new opportunities and also new challenges appear. It is necessary to plan and act together to build this new economy with care and responsibility. Below, an overview of the main digital transformations in Brazil and how to face challenges and embrace opportunities.

CNEN ANNOUNCES TEMPORARY SUSPENSION OF PRODUCTION AND SUPPLY OF RADIOPHARMACEUTICALS DUE TO CYBER INCIDENT - BRAZIL

gov.br - Last Friday, March 28, a cybersecurity incident occurred at IPEN/CNEN, which resulted in a series of attempted attacks on the Institute's network. The necessary corrective actions began on the same day and IT professionals have since been working to mitigate the causes and fully restore operations. It is important to note that physical, radiological and nuclear security were not affected. However, due to the need to preserve the integrity of the IT environment, it was necessary to disconnect the Institute's network from the external environment, including Internet access, until all necessary preventive actions were implemented.

HOW TRINIDAD AND TOBAGO IS FARING BY REGIONAL INTERNET STANDARDS

Newsday - THE INTERNET Society (ISOC) updates its Pulse rankings of countries across a range of connectivity benchmarks. ISOC is an advocacy body that supports and promotes "the development of the internet as a global technical infrastructure, a resource to enrich people's lives and a force for good in society."

THE U.S. REACTIVATES NUCLEAR POWER TO POWER ITS TECHNOLOGY DATA CENTERS.

dplnews - After having been practically banned at the end of the 20th century, in recent years—and specifically in recent months—nuclear energy has seen a resurgence. This has one origin, the United States, and one reason: the vast amount of energy its technology companies require to power their data centers. The United States is home to the largest number of data centers in the world, accounting for around a third (33%) of the global total. This makes data centers the largest contributor to the growth in electricity demand. The United States is the world's second-largest consumer of electricity, behind only China.

QUANTUM COMPUTING: A JOURNEY THAT'S JUST BEGINNING

Forbes Colombia - The development of computing has allowed humanity to achieve milestones that seemed impossible a few decades ago. From decoding DNA to performing complex astronomical simulations, the processing capacity of computer systems has evolved exponentially. Now, with quantum computing, we are on the verge of a new technological revolution that promises to transform various industries and challenge the limits of knowledge.

CYBERSECURITY REMAINS A KEY OBSTACLE TO CRYPTO ADOPTION

Forbes - Even as regulators, major financial institutions, and investors of all sizes continue to pivot and move toward embracing cryptoassets and crypto payments there is a major obstacle to wider adoption that has yet to be effectively addressed; cybersecurity concerns. While it is true that every application contains within it some level of cybersecurity risk – including that of loss – crypto and other on-chain assets remain uniquely exposed to these factors, at least as far as public opinion is concerned.

CRITICAL CONDITION: LEGACY MEDICAL DEVICES REMAIN EASY TARGETS FOR RANSOMWARE

Security Week - Healthcare is consistently one of the most attacked critical industries – it is a prime ransomware target. The reasons are clear: it offers a huge attack surface that is poorly secured in a sector that must prioritize continuous operation. It is, in short, easily compromised and most likely to pay.