DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 9, 2026

DIGI AMERICAS ALLIANCE MEMBERS

CHILE | ANCI PRESENTS ITS FIRST ANNUAL REPORT

dpl news - The National Cybersecurity Agency (ANCI) completed its initial phase at the end of 2025, marking one year since its creation and the end of the term of its first national director, Daniel Álvarez Valenzuela. With the participation of government officials, members of Congress, the judiciary, law enforcement, public services, trade associations, academia, and international representatives, the National Cybersecurity Agency (ANCI) presented its first annual report, marking a milestone in the consolidation of cybersecurity institutions in Chile.

ARGENTINA CREATES THE NATIONAL CYBERSECURITY CENTER

mobile time latino america - The Argentine government has moved forward with a comprehensive reorganization of the National Intelligence System through a decree issued on January 1, 2026. This decree introduces structural changes to cyberspace governance and establishes the National Cybersecurity Center (CNC) as the new national authority on the matter. According to an official bulletin, the measure redefines responsibilities among agencies, formally separates cybersecurity and cyber intelligence functions, and establishes a new institutional framework for the protection of critical digital infrastructure, telecommunications networks, and strategic state assets.

MEXICO PRESENTS ITS FIRST NATIONAL CYBERSECURITY PLAN, FOCUSED ON CYBER RESILIENCE AND PREVENTION

El Español - The goal of Mexico's National Cybersecurity Plan is to position Mexico at the forefront internationally as a regional leader in cyber resilience and to help reduce the risk of cyberattacks through a prevention-focused model. This landmark initiative establishes the country's first specialized cybersecurity policy framework. Presented by the ATDT (Association for the Defense of Cybersecurity), the plan aims to "standardize responses to any threat to the online infrastructure and systems of government institutions and entities." It includes a new national policy and a federal framework that will encompass mandatory measures, training for public servants, and incident reporting, among other regulations that the Mexican government hopes to publish throughout 2026.

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 9, 2026

THE BRAZILIAN ARMY WILL EXPAND ITS CYBER DEFENSE USING ARTIFICIAL INTELLIGENCE; FIND OUT HOW

Times Brasil - The Brazilian Army will receive a series of new technologies and equipment. This is because, in November 2025, Complementary Law 221 guaranteed that R$ 30 billion would be excluded from the fiscal framework and allocated to investments in Brazilian defense. Thus, throughout 2026 and 2031, the Military PAC (Growth Acceleration Program) should use R$ 3 billion each year to modernize defense resources. Therefore, in addition to a new fleet of armored vehicles, the Centauro II-BR, the army will also have an expanded cyber defense, which will include the use of artificial intelligence (AI). Below, see how AI can improve Brazilian defense.

COSTA RICA STRENGTHENS ITS POSITION AS A HUB OF GLOBAL CAPACITY CENTERS

elmundo.cr - Costa Rica continues to offer ideal conditions for establishing centers of excellence. Over the years, the country has attracted a variety of service delivery models, including Shared Services Centers (SSCs) and Global Capacity Centers (GCCs), each contributing to the development and diversification of the business services ecosystem. These centers allow multinational companies to strengthen operations, build strategic capabilities, drive innovation, and improve process quality, while optimizing responsiveness to customers across different time zones —a key element of the global follow-the-sun model that enables continuous collaboration and consistent service delivery.

CYBERSECURITY FIRM CROWDSTRIKE BUYS STARTUP SGNL FOR $740 MILLION

Infobae - Cybersecurity and technology company CrowdStrike announced Thursday an agreement to acquire the startup SGNL, which specializes in protecting artificial intelligence (AI) identities, for approximately $740 million. "We are committed to providing our customers with the technologies they need to protect all types of identities in the age of artificial intelligence," CrowdStrike stated in the press release announcing the acquisition of SGNL. The deal is valued at approximately $740 million and is expected to close in the first fiscal quarter of 2027, according to several business media outlets.

CISA ADDS TWO KNOWN EXPLOITED VULNERABILITIES TO CATALOG

CISA.gov - CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

- CVE-2009-0556 Microsoft Office PowerPoint Code Injection Vulnerability
- CVE-2025-37164 HPE OneView Code Injection Vulnerability

These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise. Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities established the KEV Catalog as a living list of known Common Vulnerabilities and Exposures (CVEs) that carry significant risk to the federal enterprise. BOD 22-01 requires Federal Civilian Executive Branch (FCEB) agencies to remediate identified vulnerabilities by the due date to protect FCEB networks against active threats. See the BOD 22-01 Fact Sheet for more information.

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 9, 2026

ENHANCING PORT SECURITY: FIVE ESSENTIAL STRATEGIES FOR LATIN AMERICA

Maritime Fair Trade - Latin America's ports are grappling with significant security challenges, heavily influenced by rising drug-related violence and cyber threats. The region has seen a surge in criminal activities linked to its ports, most notably with Ecuador's Guayaquil where drug gangs are engaging in violent turf wars. Chile has similarly experienced increased crime tied to port activities. A 2021 report by the Organization of American States (OAS) reveals that ports in the Western Hemisphere are vulnerable to cyberattacks due to rapid digitalization. These attacks, often involving ransomware, can paralyze operations, as illustrated by the 2017 NotPetya incident that caused substantial financial losses for Maersk.

COMPLEX ROUTING, MISCONFIGURATIONS EXPLOITED FOR DOMAIN SPOOFING IN PHISHING ATTACKS

Security Week - Threat actors have been observed abusing complex routing and improperly configured spoof protections in phishing attacks, Microsoft warns. By spoofing legitimate domains, the attackers make their phishing emails more effective, as they appear to have been sent internally. The attack vector, Microsoft says, has been used in opportunistic campaigns powered by phishing-as-a-service (PhaaS) platforms such as Tycoon2FA, targeting several industries. The phishing messages contain lures related to document sharing, HR communication, invoices, password resets, and voicemails, leading to the compromise of credentials that may be abused for business email compromise (BEC) or data theft.

HOW CYBER WARFARE IS BECOMING THE FIRST STRIKE IN MODERN CONFLICTS

The Street - The pre-dawn raid that saw U.S. special operations forces seize President Nicolás Maduro of Venezuela and his wife, Cilia Flores, reportedly began with cyber-attacks that cut off power to large areas of the South American country's capital city to allow planes and helicopters to strike key military sites. President Donald Trump suggested that the U.S. used cyberattacks or other technical capabilities to cut power off in Caracas, according to Politico. Last month, Venezuelan national oil and gas company PDVSA, or Petróleos de Venezuela, S.A., accused the U.S. government of carrying out a cyberattack that led to delays in operations across the country. Whether or not cyberattacks were the decisive factor in Caracas, the episode highlights how digital warfare has become a standard opening move in modern conflicts.

CLOUDFLARE POURS COLD WATER ON 'BGP WEIRDNESS PRECEDED US ATTACK ON VENEZUELA' THEORY

The Register - Cloudflare has poured cold water on a theory that the USA's incursion into Venezuela coincided with a cyberattack on telecoms infrastructure. The theory came from red team engineer Graham Helton who, on his personal blog noted that President Trump said the USA used "certain expertise" to turn off lights in the Venezuelan city of Caracas before the attack, and that the chairman of the Joint Chiefs of Staff, general Dan Caine, said US Cyber Command played a role too. "While we can't say with certainty what caused this route leak, our data suggests that it's likely cause was more mundane," Herdes wrote. "That's in part because BGP route leaks happen all of the time, and they have always been part of the Internet — most often for reasons that aren't malicious."