DIGI AMERICAS ALLIANCE MEMBERS

THE GOVERNMENT LAUNCHES A NEW INTELLIGENCE SYSTEM - ARGENTINA

The government plans to launch a new "national intelligence system" in the coming days to integrate information from key sectors of the economy and international disputes, creating a foundation for "improving strategic analysis," an official source connected to the area told El Observador. "An information network of state agencies will be established, providing the SIDE (State Intelligence Secretariat) with relevant data, although it will not produce intelligence in the strict sense," the source explained. The source clarified that cybersecurity and network protection (the responsibility of the Innovation Secretariat, under the Chief of Staff's office) will be clearly distinguished from cyber intelligence, which aims to "obtain strategic knowledge from cyberspace for decision-making."

ANCI PUBLISHES IN THE OFFICIAL GAZETTE A SET OF NEW GUIDELINES FOR OIV AND ESSENTIAL SERVICES - CHILE

TrendTIC - The implementation of the Cybersecurity Framework Law continues to advance with greater regulatory precision. In this context, the National Cybersecurity Agency (ANCI) has formalized a new set of general instructions that strengthen both the operational and governance aspects that public and private institutions providing essential services or classified as Vital Importance Operators must comply with. These are General Instructions No. 2, No. 3, and No. 4, published in the Official Gazette, which consolidate the transition from a declarative approach to a fully enforceable one in cybersecurity matters.

NEW ANATEL REGULATION RAISES THE SECURITY BAR FOR TECHNOLOGY PROVIDERS - BRAZIL

InforChannel - Since November 26th, the Brazilian telecommunications sector has entered a new phase with the mandatory independent audit of the Cybersecurity Policy (PSC) for all suppliers of telecommunications products and equipment serving operators in the country. Established by the National Telecommunications Agency (Anatel) through Act No. 16,417, published on November 26, 2024, the measure establishes a new level of responsibility and traceability for devices that integrate telecommunications networks in Brazil.

BRAZIL: BCB AND CMN ESTABLISH ADDITIONAL CYBER SECURITY REQUIREMENTS

Global Compliance News - On 18 December 2025, the Central Bank of Brazil (BCB) published National Monetary Council (CMN) Resolution No. 5,274/2025 and BCB Resolution No. 538/2025, both amending previous rules on cybersecurity and requirements for contracting cloud processing, storage and computing services for institutions regulated by the BCB. CMN Resolution No. 5,274/2025 amends CMN Resolution No. 4,893/2021, while BCB Resolution No. 538/2025 amends BCB Resolution No. 85/2021.

COLOMBIA IS MOVING TOWARDS AI-POWERED PREDICTIVE CYBERSECURITY BY 2026

Prensario TI Latin America - Cybersecurity in Colombia is preparing for a profound structural change. According to an analysis by SISAP, a regional company specializing in information security, the country is entering a new phase in which digital protection will shift from being primarily reactive to becoming predictive and autonomous, driven by artificial intelligence (AI) and advanced automation. During 2025, organizations focused their efforts on mitigating threats such as advanced phishing, credential exposure, social engineering, and third-party attacks. However, the scenario by 2026 will mark a definitive turning point. Cybercriminals are already adopting offensive AI—that is, autonomous agents capable of analyzing, deciding, and executing attacks without human intervention—which accelerates the pace and significantly raises the level of sophistication of digital crime.

AUTHORITIES ARE INVESTIGATING DAMAGE TO AN UNDERWATER TELECOMMUNICATIONS CABLE IN THE GULF OF FINLAND

Cadena3 - Authorities are investigating damage to an underwater telecommunications cable in the Gulf of Finland that occurred early Wednesday between the capitals of Finland and Estonia. Finnish authorities seized and inspected the vessel suspected of causing the damage, the border guard said in a statement. Its anchor was down when it was discovered in Finland's exclusive economic zone. Helsinki police have opened an investigation for possible aggravated criminal damage, attempted aggravated criminal damage, and aggravated interference with telecommunications. The cable belongs to the telecommunications service provider Elisa and is considered critical underwater infrastructure. The damage occurred in Estonia's exclusive economic zone, according to police. "Finland is prepared for security challenges of various kinds, and we respond to them as needed," Finnish President Alexander Stubb wrote on the social media platform X. Estonian authorities are cooperating with their Finnish counterparts to decide whether to initiate a separate criminal case or proceed with a joint prosecution.

CYBERSECURITY AND THE TECHNOLOGICAL TSUNAMI OF 2026: THE COLLISION BETWEEN AI, QUANTUM COMPUTING AND WEB 4.0

Portal Innova - The year 2026 will not be defined by gradual upgrades. It will be marked by an unprecedented collision of forces: next-generation computing, hyperautomation, and a global reckoning in cybersecurity. According to Check Point Software Technologies, the coming landscape is anticipated in the following ten predictions.

WHY RUSSIAN HACKERS ARE ABANDONING ZERO-DAYS FOR MISCONFIGURATIONS

Security Buzz - For years, elite state-backed hackers have been defined by their exploits. Zero-days were the calling card—rare bugs, complex chains, techniques that only a handful of teams could pull off. That image still dominates how many defenders think about top-tier threats. Amazon's latest threat intelligence challenges that assumption. According to AWS, Russian state-sponsored attackers tied to Sandworm are increasingly gaining access through misconfigured network edge devices, exposed management interfaces, and cloud environments with overly permissive settings. These attackers haven't lost the ability to exploit software; they've simply chosen not to. If misconfigurations get them in quietly and with little risk, there's no reason to burn a valuable exploit.

CARETO HACKER GROUP IS BACK AFTER 10 YEARS OF SILENCE WITH NEW ATTACK TACTICS

Cybersecurity News - After a decade of disappearing from the cybersecurity landscape, the Careto threat group, also known as "The Mask," has resurfaced with sophisticated new attack methods targeting high-profile organizations. Security researchers have identified fresh evidence of Careto's activity, revealing how the group evolved its tactics to compromise critical infrastructure and maintain persistent access to sensitive networks. The Careto group has been conducting advanced cyberattacks since at least 2007, traditionally focusing on government agencies, diplomatic entities, and research institutions. Careto aka The Mask resurfaces after a decade, launching advanced attacks on high-profile targets and critical infrastructure.

TELECOM OPERATORS' CYBERSECURITY SPENDING TO HIT $42B IN SIX YEARS

The Guardian - The Groupe Spéciale Mobile Association (GSMA) has warned that fragmented cybersecurity regulation is raising costs and increasing mobile operators' risk. GSMA, in a new independent study titled "The Impact of Cybersecurity Regulation on Mobile Operators," revealed that mobile operators are spending between $15-19 billion yearly on core cybersecurity activities, a figure expected to rise to $40-42 billion by 2030. Despite this significant investment, the telecom body said mobile network operators, which form the backbone of digital economies worldwide, are impacted by poorly designed, misaligned or overly prescriptive regulation, which results in unnecessary costs, diverting resources from genuine risk mitigation, and in some cases increasing exposure to cyber threats.

WHAT EVERY COMPANY NEEDS TO KNOW ABOUT CYBERSECURITY IN 2026

Forbes - 2026 is a pivotal juncture for cybersecurity. What was once considered an operational safety net and a business cost item is now a determinant of long-term competitiveness, market confidence, and organizational resilience. The data unequivocally indicates that cyber danger is systemic rather than episodic. The difficulty facing firms in 2026 is not whether to invest in cybersecurity, but rather how to integrate it with governance, corporate strategy, and operational continuity.