DIGI AMERICAS LATAM CISO

INSIGHTS

NOVEMBER 6, 2025

DIGI AMERICAS ALLIANCE MEMBERS

Apple aws Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks we hack your software

Google kriptos LUMU netskope paloalto NETWORKS Resecurity

Schneider Electric SISAP Sistemas Aplicativos Strike Telefónica tenable Trellix TREND MICRO

DOMINICAN REPUBLIC | INDOTEL PROMOTES CYBERSECURITY TRAINING AFTER ONE BILLION ATTEMPTED CYBERATTACKS IN ONE YEAR

DPL News - The president of the Board of Directors of the Dominican Institute of Telecommunications (Indotel), Guido Gómez Mazara, stated that the regulatory body is promoting cybersecurity training programs to ensure that the Dominican Republic remains a secure country in terms of technology and the protection of digital data.

PANAMA STRENGTHENS ITS DIGITAL DEFENSE AGAINST THE WAVE OF GLOBAL CYBERATTACKS

La Estrella de Panama - In response to the increase in cyberattacks worldwide, Panama is advancing in the protection of its critical systems with cybersecurity solutions, including automation and artificial intelligence, to guarantee operational continuity and regulatory compliance. The cyber threat is intensifying. In recent months, sophisticated attacks have shaken airports, factories, and the security of millions of users. Hackers are leveraging artificial intelligence and advanced social engineering techniques, expanding the attack surface to critical sectors such as education, energy, and aviation.

DEBATERS PRAISE AND MAKE SUGGESTIONS FOR THE CYBERSECURITY LEGAL FRAMEWORK - BRAZIL

Senate Agency - In a public hearing promoted by the Parliamentary Front for Support of Cybersecurity and Cyber Defense on Tuesday afternoon (4), experts praised and made suggestions to the Cybersecurity Legal Framework project (PL 4.752/2025). The author of the project is Senator Esperidião Amin (PP-SC), who is also the president of the parliamentary front. He chaired the hearing. The senator informed that the project is still awaiting the appointment of a rapporteur in the Constitution and Justice Committee (CCJ). And he suggested that the rapporteurship be given to a senator who is a member of the front.

WILL ANATEL TAKE OVER CYBERSECURITY REGULATION IN BRAZIL?

DPL News – Lacking the budgetary resources to create a new autonomous agency, the Institutional Security Cabinet (GSI) of the Brazilian Presidency has decided to propose that the National Telecommunications Agency (Anatel) assume the role of central body for the federal government's cybersecurity policy. This change is included in the new version of the draft bill currently being debated by the National Cybersecurity Committee (CNCiber). The head of the GSI, General Marcos Antonio Amaro dos Santos, explained that the initiative aims to give national scope to the Cybersecurity Policy and Strategy—approved in 2023 and 2025, respectively.

HOW SOCS ADDRESS CYBER THREATS IN BRAZIL

According to data from Febraban (Brazilian Federation of Banks), 100% of Brazilian banks consider information security a top priority, reflecting a trend that extends to other critical sectors of the economy. Simultaneously, the national IT sector is growing at rates exceeding 9% annually, including investments in security, monitoring, and digital infrastructure. SOCs (Security Operations Centers) not only monitor and detect incidents in real time but also structure rapid and coordinated response processes, reducing financial and reputational impacts. However, maintaining a robust internal SOC requires significant investments in technology and specialists, creating space for the growth of the SOCaaS (SOC as a Service) model, which combines external expertise, automation, and artificial intelligence.

CYBERSECURITY EXPERTS MANAGED TO BLOCK MORE THAN 5,000 BANK ATTACKS IN CHILE, AND ALSO OBSERVED AN INCREASE IN THREATS TARGETING SMARTPHONES

TrendTIC – According to a recent report by a cybersecurity firm, 1.8 million banking Trojan attacks were blocked between August 2024 and June 2025—an average of about 5,000 per day. Despite a nearly 55.5% decrease compared to the previous year (3.3 million), the threat has not diminished, it has only transformed. In Chile alone, more than 5,000 attacks were blocked. The report indicates a shift in cybercriminals' approach: attacks are migrating from computers to mobile devices, following the increased use of smartphones for financial transactions.

ARGENTINA OUTLINES SCIENCE, TECHNOLOGY AND INNOVATION GUIDELINES FOR 2027

DPL News – The Argentine government has officially released the roadmap for the next two years of its National Science, Technology and Innovation Plan 2030 (PNCTI2030). Resolution 282/2025, published by the Secretariat of Science, Technology and Innovation (SICyT), outlines the guidelines for the 2025-2027 period. The document prioritizes promoting four strategic sectors: Agroindustry, Energy and Mining, Knowledge Economy and Innovation, and Health, considering them to have “high economic and social impact, with the capacity to generate skilled employment, increase value-added exports, and strengthen the country's international competitiveness.”

FOR THE FIRST TIME IN A PROVINCIAL LEGISLATURE: THE REGIONAL PARLIAMENTARY SUMMIT ON AI AND CYBERSECURITY IS HELD

The Córdoba Legislature is hosting the 3rd Regional Parliamentary Summit, “Forging Digital Futures in the Southern Cone: AI, Innovation, Data, and Cybersecurity,” marking the first time this annual meeting has been held in a provincial legislature. Senators, representatives, and technology specialists from South and Central American countries gathered at the Córdoba unicameral legislature to discuss the challenges and opportunities presented by digital transformation and internet governance. Thematic panels will take place on Monday and Tuesday, including “Public Innovation and the Digital Transformation of the State”; “Innovation, Technology, and the Private Sector — The Role of Companies in the AI and Sustainable Development Agenda”; and “Emerging Technologies and Innovation: Opportunities and Risks.” Participants from Argentina, Paraguay, Uruguay, Costa Rica, Panama, and Mexico, among other countries, will share their experiences.

US PROSECUTORS SAY CYBERSECURITY PROS RAN CYBERCRIME OPERATION

Reuters - Prosecutors said three American cybersecurity professionals secretly ran a ransomware operation aimed at shaking down companies across the United States. The three people, only two of whom - Ryan Goldberg and Kevin Martin - were identified by name, collaborated with the notorious hacking gang ALPHV BlackCat to encrypt companies' networks in a bid to extort their owners out of millions of dollars' worth of cryptocurrency, prosecutors alleged in an indictment filed last month, opens new tab in federal court in Miami.

HOW PETS HELP BANKS PROTECT CONSUMERS FROM FRAUD WITHOUT SHARING PERSONAL DATA

WEF - Fraud is rising, but collaboration between banks can reverse this trend. Privacy-enhancing technologies (PETs) let organizations derive insights together while keeping raw data under each party’s control. PETs enable banks to collaborate in ways that respect privacy and deliver the protection consumers expect. Fraud keeps climbing. In the United States alone, consumers reported more than $12.5 billion in losses in 2024, up about 25% year-over-year. Behind that figure are victims whose savings were drained, whose credit scores were destroyed by fraudulent loans, and whose stolen identities continue to cause harm long after the initial incident.

CYBERCRIMINALS EXPLOIT REMOTE MONITORING TOOLS TO INFILTRATE LOGISTICS AND FREIGHT NETWORKS

The Hacker News - Bad actors are increasingly training their sights on trucking and logistics companies with an aim to infect them with remote monitoring and management (RMM) software for financial gain and ultimately steal cargo freight. The threat cluster, believed to be active since at least June 2025 according to Proofpoint, is said to be collaborating with organized crime groups to break into entities in the surface transportation industry with the end goal of plundering physical goods. The most targeted commodities of the cyber-enabled heists are food and beverage products. "The stolen cargo most likely is sold online or shipped overseas," researchers Ole Villadsen and Selena Larson said in a report shared with The Hacker News. "In the observed campaigns, threat actors aim to infiltrate companies and use their fraudulent access to bid on real shipments of goods to ultimately steal them."