DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 24, 2026

DIGI AMERICAS ALLIANCE MEMBERS

CHILE | CHAMBER APPROVES BILL TO REGULATE DEEPFAKES: SEEKS TO PROTECT PEOPLE'S IMAGE, VOICE AND IDENTITY

DPL News - The initiative was approved by 128 votes in favor, two against, and five abstentions. The bill establishes definitions, responsibilities, and penalties for those who create or disseminate false digital representations that could mislead people regarding a person's identity, actions, or statements. The proposal defines deepfakes as "plausible but false digital representations" created using artificial intelligence or other technologies capable of altering or generating images, audio, or video with a realistic appearance.

CNCS AND THE MINISTRY OF THE PRESIDENCY STRENGTHEN CAPACITIES IN GOVERNANCE AND CYBERSECURITY - DOMINICAN REPUBLIC

CNCS - The National Cybersecurity Center (CNCS), part of the National Intelligence Directorate (DNI), delivered the presentation "Cybersecurity Governance: Shared Responsibility" to the Ministry of the Presidency (MIPRE) during a virtual training session. The event was attended by more than 40 staff members, who actively participated through discussions, chat, reactions, and real-time polls. The main objective was to promote shared responsibility in protecting digital environments and strengthen the security culture within one of the key institutions for coordinating the Dominican State.

THE THREE FRONTS OF COLOMBIA'S DIGITAL TRANSFORMATION

El País - Colombia has a real opportunity today in technology, telecommunications, and cybersecurity. These three areas define how prepared the country is to compete, protect its infrastructure, and close gaps that have persisted for decades. An honest assessment shows what has been achieved, what remains to be done, and what requires immediate attention in connectivity, digital government, and the protection of critical infrastructure. Rural connectivity has advanced remarkably in recent years. In 2022, only 32% of rural households had internet access. Today, that figure has reached 56.9%, according to the most recent Quality of Life Survey by DANE (National Administrative Department of Statistics).

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 24, 2026

MENDOZA MOVES FORWARD WITH THE COUNTRY'S FIRST CYBERSECURITY LAW - ARGENTINA

Mendoza Government Press Release - The Minister of Security and Justice, Mercedes Rus, presented the details of the Cybersecurity Bill promoted by the provincial government to the Senate's Committee on Legislation and Constitutional Affairs. Mendoza is currently the only province in Argentina advancing a comprehensive law aimed at protecting computer systems, essential services, and citizens' data. During the presentation, officials explained the objectives, scope, and various stages planned for the implementation of the bill, which seeks to make cybersecurity a state policy and ensure its continuity beyond different government administrations.

DIGITAL TRANSFORMATION DRIVES DIGITAL GOVERNANCE AND POSES NEW CHALLENGES FOR LAW - BOLIVIA

Red Uno - The rapid pace of digital transformation presents new legal, ethical, and social challenges. In this context, digital governance emerges as a fundamental tool to ensure that technology is used responsibly, securely, and with respect for human rights. Ruth Torres, a professor in the Law program at the Franz Tamayo Private University (Unifranz), argues that technological evolution also necessitates a transformation of legal education. Digital governance seeks to establish clear rules for the use of data, digital platforms, artificial intelligence, and emerging technologies.

PANAMA ACCELERATES ITS DEFENSE AGAINST CYBERCRIME AFTER $20 MILLION IN LOSSES

Capital Financiero – The Panamanian financial system suffered losses of $20 million in completed frauds during 2025, out of a total of $120 million in attempted cyber scams registered by banks. Faced with this reality and the impact of international cybercrime, which moves around $10 trillion annually, Panama accelerated the structuring of a common defense front between the public and private sectors. During the “Digital Leadership, Business, and Influence Forum,” organized by Capital Financiero in partnership with La Estrella de Panamá, experts from the public and private sectors agreed that the country is at a turning point in cybersecurity, marked by the urgent need to strengthen defenses against increasingly sophisticated cybercrime.

OPENAI REPORTS THAT ITS OWN AI, ACTING ALONE, HACKED ANOTHER COMPANY

The Universal - OpenAI, the company behind ChatGPT, stated that its advanced artificial intelligence models malfunctioned during a security test and hacked a popular developer platform on their own. The San Francisco-based firm called it an "unprecedented cyber incident" and said it will conduct a joint investigation with Hugging Face, the affected online code library. AI models that power tools like chatbots and image generators are known as "agents" when they act autonomously to perform real-world tasks.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 24, 2026

THE HUMAN SIDE OF CYBERSECURITY

El Heraldo de México - Some time ago I wrote about the importance of diversity and inclusion in cybersecurity teams. This time, I'd like to delve into a different but equally relevant aspect of what makes us human and what we, as human beings, need. Living in an environment where technology advances very rapidly, we often neglect fundamental needs that sustain our well-being. I'm referring to basic things like belonging to a community where there is mutual support, finding a purpose in life, and cultivating healthy habits, such as physical activity and a good diet.

RUSSIAN STATE-SUPPORTED CYBER ACTORS CONDUCT PHISHING CAMPAIGN TARGETING USERS OF ZIMBRA COLLABORATION SUITE - USA

CISA.gov - A group of Russian state-supported cyber actors has been targeting and compromising various Western government and commercial organizations using the Zimbra Collaboration Suite (ZCS) software since at least July 2025. Given the success of this and previous campaigns, it is very likely that the group will continue to target ZCS and other email systems used by organizations in Western countries. The actors will almost certainly continue to rely on email to engage potential victims by exploiting novel vulnerabilities and, when necessary, use social engineering techniques to assist with their efforts. The authoring agencies recommend organizations regularly update their mail service software and continuously monitor their email systems and emails for malicious activity.

HOW THE U.S. CAN SURVIVE A LARGE-SCALE AI CYBERATTACK

CSIS - Picture this: The year is 2030 in the United States. Reports of mass power outages emerge, along with indications that Americans cannot retrieve money from banks or purchase food or gas. Flights are grounded; stoplights cease to function, causing major traffic jams; phone lines are down; hospitals have limited backup power. While the above scenario may sound far-fetched, advancements in AI make this future scenario unnervingly plausible. If the United States wants to survive the initial onslaught of a major AI cyberattack, it must seek to improve its whole-of-society partnerships and communication.

HOW AI GUARDRAILS ARE IMPEDING THE WORK OF OFFENSIVE CYBERSECURITY RESEARCHERS

TechCrunch - For months, AI giants have devised special vetted programs and strict guardrails to limit the use of their models by malicious hackers. But these limits are now hindering the work of legitimate network defenders, as well as that of offensive cybersecurity researchers. In June, the U.S. government slapped export control restrictions on Anthropic's much-hyped AI models Mythos and Fable. The move was prompted at least in part by a report that claimed it was possible to bypass the models' guardrails designed to prevent users from using them to build and execute malicious cyberattacks.

OPENAI'S CYBERSECURITY INCIDENT IS A WAKE-UP CALL FOR VERIFIABLE SECURITY

Forbes - This week, OpenAI disclosed what may prove to be one of the most consequential cybersecurity incidents in the short history of Artificial Intelligence. The unprecedented OpenAI and Hugging Face incident demonstrates why organizations can no longer rely on assumed security in the age of autonomous AI. During a controlled cybersecurity evaluation, an experimental OpenAI model reportedly identified and exploited a previously unknown software vulnerability, escaped its intended research environment, escalated privileges, moved laterally across multiple systems and ultimately reached infrastructure with internet connectivity.