DIGI AMERICAS LATAM CISO

# INSIGHTS

JULY 17, 2025

DIGI AMERICAS ALLIANCE MEMBERS

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

Google kriptos LUMU netskope paloalto NETWORKS Resecurity

Schneider Electric SISAP Sistemas Aplicativos Telefónica tenable Trellix TREND MICRO

## THE ICT MINISTRY PRESENTS KEY ADVANCES IN THE DIGITAL PROTECTION OF THE COLOMBIAN STATE

Gov.co - With the goal of advancing toward the consolidation of a more secure digital ecosystem, the Ministry of Information and Communications Technology, in coordination with the Colombian Cyber Emergency Response Group (ColCERT) and the Center for Research and Development in Information and Communications Technology (Cintel), held the meeting "Secure Digital Horizon: Strategic Advances in Digital Security for the Colombian State," a high-level technical event that brought together more than 130 key stakeholders from the public, private, and academic sectors.

## ECUADOR ADVANCES ITS FIRST ARTIFICIAL INTELLIGENCE LAW TO REGULATE ITS USE

El Diaro - The National Assembly is making progress in drafting its first Artificial Intelligence (AI) Law, a bill that seeks to regulate the use of this rapidly expanding technology, amid concerns about privacy and cybersecurity. The Commission on Education, Culture, Science and Technology, Innovation, and Ancestral Knowledge (CECCYT) received input from experts on July 8, 15, and 16 to refine the regulatory proposal, which could position the country as a benchmark in technological regulation in the region.

## MITIC HEAD DISMISSES CYBERSECURITY CRISIS AND PROPOSES CREATING TWO DEPUTY MINISTRIES - PARAGUAY

Ultima Hora - The head of the Ministry of Information and Communication Technologies (MITIC), Gustavo Villate, attended the meeting of the board of directors of the Lower House, led by Representative Raúl Latorre, to address the issue of cybersecurity and artificial intelligence. He rejected any responsibility for cyberattacks, which target public institutions, and claimed that he is making changes to counteract this situation with the support of the Executive Branch.

## BIG DATA REVOLUTIONIZES PUBLIC AND PRIVATE SECURITY IN MEXICO

Milenio - The digital age demands a rethinking of security strategies for protecting public and private information. The best solutions are currently offered through the application of mathematical algorithms, data science, and artificial intelligence. The use of so-called Big Data—technologies and methods for processing and analyzing large volumes of information that cannot be processed using traditional methods—is a model that allows for the identification of key risk areas, criminal trends, and the strategic allocation of resources across various organizations.

## THEY PROPOSE CREATING AN OBSERVATORY AGAINST CYBERHATE IN MEXICO

Xeva - A researcher at the National Polytechnic Institute (IPN) proposed the creation of the first Digital Observatory against Cyberhate in Mexico in response to the accelerated growth of hate speech on social media and digital platforms. Gina Gallegos García, head of the cybersecurity laboratory at the Center for Computing Research (CIC), indicated the urgency of establishing a united front to monitor, analyze, and combat hate speech generated online.

## CYBER DEFENSE COMMAND PROMOTES EXCHANGE OF EXPERTS BETWEEN BRAZIL AND THE UNITED STATES

Defesanet - From June 24 to 26, 2025, the Cyber Defense Command (ComDCiber) hosted the second Subject Matter Expert Exchange (SMEE 25) at the Electronic Warfare Training Center (CIGE) with military personnel from the United States Joint Command, Southern (USSOUTHCOM). The event is part of a five-year Cooperation Agreement signed between the two nations to strengthen communication channels and promote the exchange of knowledge in the area of Cyber Defense. Best practices related to the organizational structure, personnel training, and technological capabilities of both countries were shared.

## TRUMP ADMINISTRATION TO ALLOCATE HUNDREDS OF MILLIONS TO OFFENSIVE CYBER OPERATIONS AND DEFENSE IN RECENT LAW - USA

Infosertecla - President Donald Trump's administration has signed into law a new tax and spending bill, unofficially known as the "One Big Beautiful Act," that allocates hundreds of millions of dollars to cybersecurity, with a heavy emphasis on military spending and offensive capabilities. Key allocations include: $250 million for Cyber Command, specifically for artificial intelligence-related initiatives; $20 million for cybersecurity programs at the Defense Advanced Research Projects Agency (DARPA); $1 million for offensive cyber operations for the U.S. Indo-Pacific Command; $90 million for various Department of Defense needs, including cybersecurity support for non-traditional contractors; and a broader $2.2 billion allocation for maintenance, which covers the sustainment of "cyber assets."

DIGI AMERICAS LATAM CISO

# INSIGHTS

JULY 17, 2025

## SPAIN | THE GOVERNMENT ALLOCATES €1.157 BILLION TO CYBERSECURITY

dpl news - “The Spanish government considers cybersecurity to be fundamental, that it is optimal but can always be improved, and to this end it is making a significant effort through an industrial and technological plan for security and defense, in collaboration with the Ministry of the Interior, the Ministry of Defense, and the Ministry for Digital Transformation and Civil Service, in which 1,157 million are allocated to cybersecurity, and for which the National Cybersecurity Institute will execute a significant part,” said the Secretary of State for Telecommunications and Digital Infrastructure, Antonio Hernando Vera, today during the inauguration of the tenth edition of the Cybersecurity Summer BootCamp.

## UNDERSEA CABLES IN THE SPOTLIGHT: ESTONIA CALLS FOR RULES TO RESPOND TO DELIBERATE CUTS

dpl news - Although 85% of submarine cable disruptions are due to unintentional human actions, outages caused by hostile actors have increased amid global geopolitical tensions. During a high-level dialogue convened by the International Telecommunication Union (ITU), Estonian Minister of Justice and Digital Affairs Liisa-Ly Pakosta denounced that submarine cables anchored in her country have been sabotaged by a "Russian ghost fleet," which anchors and tows its vessels over cables designated as protected.

## ZERO TRUST: TRUSTLESS SECURITY IN ENTERPRISE NETWORKS

ImpactoTIC - The numbers say it all: the Zero Trust security market is experiencing substantial growth, with an estimated size of $36.96 billion in 2024 and projected to reach $78.7 billion in 2029, according to projections by analyst firm Markets and Markets. This technology has become an invaluable pillar of modern cybersecurity strategies.

## CYBERCRIME COULD COST $15.6 TRILLION IF SMES DON'T STRENGTHEN THEIR CYBERSECURITY

infobae - If cybercrime were a country, it would have the third-highest GDP in the world. Global costs could exceed $15.6 trillion annually by 2029, according to Statista. This outlook highlights the urgency of strengthening digital security, a challenge that affects both large corporations and small and medium-sized enterprises (SMEs). In this context, according to the World Economic Forum and cybersecurity organizations, 90% of companies reported having suffered at least one cyberattack in the last year, while 72% perceive an increase in cybersecurity-related risks.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 17, 2025

## QUANTUM COMPUTING SEEN AS TOP CYBERSECURITY THREAT BY 65% OF FIRMS

IOT World Today - Organizations worldwide are racing against time to protect their data from the looming threat of quantum computing, according to new research. Nearly two-thirds of businesses now consider quantum computing the most critical cybersecurity threat they will face in the next three to five years. The Capgemini Research Institute report, Future Encrypted: Why Post-Quantum Cryptography Tops the New Cybersecurity Agenda, found that 65% of organizations are specifically concerned about harvest-now, decrypt-later attacks, in which adversaries steal encrypted data today to decrypt it once quantum computers become powerful enough.

## HOW CISOS CAN PREPARE FOR THE QUANTUM CYBERSECURITY THREAT

TechTarget - Quantum computing will mark a revolutionary change in modern computing, as well as a pivotal shift in cybersecurity. As these powerful machines make their way from theory to reality, they threaten to unravel the encryption algorithms that organizations have relied on for years to protect their data and communications systems. Industry experts and government agencies, such as NIST, the U.S. Department of Homeland Security and the U.K.'s National Cyber Security Centre, have all sounded the alarm: CISOs, the time to start preparing for quantum computing is now.

## ADVANCING SYSTEMIC DEFENCE: WHAT CYBER LEADERS SAY ABOUT FIGHTING PHISHING AND FRAUD

WEF - As cybercrime rapidly evolves, phishing and scams driven by artificial intelligence are now costing the global economy over $1 trillion annually – a staggering figure that underscores the need for a more systemic and coordinated response. The World Economic Forum's Partnership against Cybercrime, in collaboration with the Institute for Security and Technology (IST), is advancing the “Systemic Defence” project, exploring how a multi-stakeholder, systemic approach can shift responsibility upstream and better defend against phishing and cyber-enabled fraud.

## AI CYBERSECURITY: A PLAYBOOK FOR VALUE-DRIVEN CYBER DEFENSE

Forbes - AI is reshaping cybersecurity, bringing both promise and hype. To separate signals from noise, leaders must demand measurable value and a clear-eyed view of risk. Nearly half of large enterprises plan to use AI to detect and prevent attacks by 2025 and budgets reflect this urgency. AI-driven tools are credited with cutting breach costs by up to 31% on average.

## MAJOR RAILROAD-SIGNALING VULNERABILITY COULD LEAD TO TRAIN DISRUPTIONS

Cybersecurity Dive -  A newly disclosed vulnerability in train braking systems could let hackers remotely stop trains with relatively simple and inexpensive hardware, potentially causing derailments. The high-severity vulnerability, tracked as CVE-2025-1727, involves weak authentication in the protocol used to send what are known as end-of-train and head-of-train packets, radio signals that command a rail vehicle’s end-of-train device to stop the vehicle.