DIGI AMERICAS LATAM CISO

# INSIGHTS

JANUARY 22, 2026

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 SOPHOS tenable Trellix TREND MICRO

## DATA PROTECTION LAW IN PARAGUAY: HOW REGULATION 7593 REDEFINES CYBERSECURITY AND DIGITAL BUSINESS

LexLatin - Last year, Paraguay repeatedly made regional news with a particularly critical issue: online security. When this nation made headlines, it was for a reason: its defenses against data theft and hacking are weak, making the country an easy and recurring target for cybercriminals. This demonstrated not only the fragility of its security system but also the urgent need for legislation to address this issue.

## CYBERSECURITY IS BACK ON THE PUBLIC AGENDA IN MEXICO; THE CHALLENGE IS IMPLEMENTATION

Cronico - For years, cybersecurity in Mexico was recognized as important, but treated as a secondary issue without continuity on the national agenda. Therefore, the development of the National Cybersecurity Plan 2025-2030 and the General Cybersecurity Policy for the Federal Public Administration represents a significant shift: the State acknowledges that digital transformation is impossible without security. Both documents reintroduce cybersecurity into the public discourse with a diagnosis, a narrative, and a general roadmap. They recognize that the current environment combines digital and physical risks: organized cybercrime, geopolitical tensions, fragile supply chains, and the use of artificial intelligence to amplify attacks.

## MEXICO'S LAGS IN CYBERSECURITY AND RISKS TO ITS DIGITAL SOVEREIGNTY ARE HIGHLIGHTED

MSN - Mexico faces an increasingly complex cybersecurity landscape, with threats that could compromise everything from the operation of public institutions and businesses to the protection of personal data and the country's digital sovereignty. This warning came from specialists during the forum "Cybersecurity: Youth, Digital Sovereignty, and Technology," held at the Chamber of Deputies. At the meeting, experts urged the strengthening of the legal framework and the Mexican State's response capacity to prevent the country from remaining highly vulnerable to large-scale cyberattacks and malicious campaigns targeting its critical infrastructure.

## CYBERSECURITY GAPS PERSIST AS DIGITAL FRAUD ACCELERATES IN MEXICO

Mexico Business News - While Mexico advances in digital maturity, fraud remains the primary obstacle to digital trust. Although eight out of 10 users feel capable of protecting themselves online, nearly 80% faced scam attempts in the previous year, reveals the Global Cybersecurity Study 2025 by Mastercard. “Mexico is experiencing a historic acceleration in digital payments and financial services. This progress opens a strategic opportunity: to consolidate trust as the main driver of economic growth,” says Marcos Peralta, Vice President, Customer Solutions Center, Mastercard North Latin America. When cybersecurity is integrated from design, innovation can scale responsibly and generate sustained value for consumers, companies, and the financial system as a whole.”

## PANAMA AND JAPAN ADVANCE COOPERATION ON CYBERSECURITY AND PROTECTION OF CRITICAL INFRASTRUCTURE

ReportAsia - Panama and Japan strengthened their bilateral cooperation agenda on cybersecurity, critical infrastructure protection, and strategic sectors during a cybersecurity meeting between the two countries. The meeting, led by Acting Foreign Minister Carlos A. Hoyos, included government officials and technical teams from both nations. The meeting facilitated an exchange of perspectives and experiences on protecting strategic assets such as the Panama Canal, the national logistics platform, and infrastructure projects under development, including connectivity plans between the Caribbean and the Pacific.

## BRAZILIAN FEDERAL COURT TO USE GAMIFICATION TO TRAIN JUDGES IN CYBERSECURITY - BRAZIL

Digital Convergence - The Federal Judiciary will launch a new cybersecurity training program later this year. The initiative, entitled "Cybersecurity Exercises in the Federal Judiciary," will be promoted by the General Inspectorate of the Federal Judiciary in partnership with the Center for Judicial Studies of the Federal Justice Council. The proposal stems from the diagnosis that every computerized system will, sooner or later, be tested by failures or external attacks, and that the difference lies in the ability to respond. Instead of theoretical training, the course will rely on an innovative gamification methodology to develop practical skills. Participants will be exposed to collaborative and immersive simulations, with both in-person and distance learning activities.

## THE EU WANTS TO BAN HUAWEI AND ZTE FROM EUROPEAN TELECOMMUNICATIONS NETWORKS DUE TO “RISKS TO DEMOCRACY AND THE ECONOMY”

Infobae - The European Commission made progress on Tuesday in its intention to exclude high-risk foreign suppliers, such as Chinese technology companies Huawei and ZTE, from telecommunications networks and other critical infrastructure in member states, proposing that Brussels' 5G network security recommendations be mandatory. According to the Commission President, this package of measures is an important step in ensuring European technological sovereignty and guaranteeing "greater security for all." The EU will therefore offer all necessary means to "better protect critical infrastructure supply chains and decisively combat cyberattacks."

DIGI AMERICAS LATAM CISO

# INSIGHTS

JANUARY 22, 2026

## LEADERS IN DAVOS WARN ABOUT LATIN AMERICA'S LACK OF PREPAREDNESS FOR CYBERATTACKS

EFEcomunica – Leaders from governments, businesses, and multilateral organizations met in Davos to analyze the impact of cybersecurity on economic stability. Latin America registered the lowest level of global confidence in its ability to respond to a large-scale cyberattack, at just 13%, according to data analyzed at the World Economic Forum. In the discussion, held during a private roundtable organized by Digi Americas Alliance and hosted by Google Cloud on the sidelines of the World Economic Forum, participants agreed that cybersecurity has ceased to be a purely technical issue and has become a pillar of competitiveness, digital trust, and economic inclusion.

## UK AND CHINA REACH OUT ACROSS CYBER NO-MAN'S LAND

ComputerWeekly - The British and Chinese authorities have reached out to one another to explore setting up a cyber security forum between the two countries, according to reports. The so-called ‘cyber dialogue’ will supposedly help to manage cyber threats to both country’s national security, revealed Bloomberg, which was first to report the move citing anonymous sources with knowledge of the forum. It claimed that the forum will improve communication, enable private discussions and de-escalate tensions. It also establishes a direct line between London and Beijing to enable senior officials to discuss ongoing cyber incidents.

## CYBER THREATS ACCELERATE GLOBALLY AS AI, GEOPOLITICS, AND FRAUD RESHAPE CYBERSECURITY LANDSCAPE

babl - Cybersecurity threats are accelerating at a global scale, driven by rapid advances in artificial intelligence, geopolitical volatility, and a sharp rise in cyber-enabled fraud, according to the World Economic Forum’s “Global Cybersecurity Outlook 2026” report. The annual survey of CEOs, CISOs, and cybersecurity leaders finds that emerging technologies are expanding both attack surfaces and defensive capabilities, producing what analysts describe as a “cyber arms race.” The report warns that AI has become the most significant force shaping cyber risk, with 94% of surveyed organizations identifying it as the leading driver of change in 2026. Adoption cuts both ways: organizations are deploying AI to automate detection and response, yet attackers are using the same tools to enhance phishing, reconnaissance, and social engineering. At the same time, 87% of respondents reported that AI-related vulnerabilities grew faster in 2025 than any other cyber risk, underscoring rising concerns over data exposure and adversarial capabilities.

## AI VS. AI IS THE NEW SECURITY BATTLEGROUND

Fierce Network - Telcos and enterprises must prepare for emerging security threats posed by AI in the hands of attackers, part of a broader trend toward industrialized cybercrime. As the security landscape changes, the role of telcos and other communications service providers is growing. CSPs must move beyond simple connectivity to securing the entire ecosystem of 5G, AI and IT and OT technologies. Ian Swanson, Palo Alto Networks VP of AI security noted unauthorized action is eclipsing data leakage as the primary threat to organizations. "These agents require deep integration into our IT ecosystems to do their jobs. They connect directly to APIs, SaaS platforms and databases. That means a successful attack triggers real consequences."