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 TrendAI

THE DOMINICAN REPUBLIC STRENGTHENS ITS REGIONAL LEADERSHIP IN DIGITAL TRANSFORMATION THROUGH PUBLIC INVESTMENT AND INTERNATIONAL COLLABORATION

Infobae – The challenges of digital transformation in Latin America demand the construction of state-of-the-art infrastructure and ensuring that its impact reaches all segments of the population, especially in rural areas and marginalized cities. The case of the Dominican Republic illustrates how comprehensive strategies can be implemented that achieve measurable progress in connectivity, inclusion, and the development of digital skills.

ANPD GAINS AUTONOMY AND STRENGTHENS CONTROL OVER THE USE OF DATA ON THE INTERNET - BRAZIL

Fast Company Brazil - The Senate approved last Tuesday (24), in Brasília, the provisional measure that transforms the National Data Protection Authority into the National Data Protection Agency (ANPD). The proposal was voted on the eve of the end of its validity period and received approval in the form of a conversion bill. The change occurs to strengthen the structure of the body responsible for overseeing the use of data in the country. According to the Senate, this change allows the regulation of the Digital Statute of the Child and Adolescent (ECA), which comes into effect in March. The matter now goes to presidential sanction.

BILL PROPOSES TAX INCENTIVES TO STRENGTHEN CYBERSECURITY OVERSIGHT - BRAZIL

Digital Capital - Bill 246/2025, authored by Senator Mecias de Jesus, is currently being processed in the Federal Senate. It proposes changes to the conditions under which foreign cybersecurity companies can access reduced rates for the Tax on Goods and Services (IBS) and the Contribution on Goods and Services (CBS). Currently, Complementary Law 214 establishes a 60% reduction in IBS and CBS rates for cybersecurity companies, provided they have a Brazilian partner holding at least 20% of the company's shares.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 26, 2026

BRAZIL AND SOUTH KOREA STRENGTHEN BILATERAL COOPERATION ON CRITICAL MINERALS

Business Moment - President Luiz Inácio Lula da Silva's state visit to Seoul on Monday (23) marked a new chapter in diplomatic relations between Brazil and South Korea. In a summit meeting with South Korean President Lee Jae-myung, the leaders sealed a commitment to elevate the bilateral relationship to the level of a strategic partnership. The meeting, which takes place 21 years after the last official visit of a Brazilian president to the country, resulted in the signing of ten memoranda of understanding (MoUs) covering areas ranging from the exploration of critical minerals to cooperation in artificial intelligence and cybersecurity.

SECOND BUDAPEST PROTOCOL: COLOMBIA PREPARES RULES FOR CROSS-BORDER DIGITAL TESTING

ImpactoTIC Colombia – The Ministry of Information and Communications Technologies (MinTIC), the Colombian Cyber Emergency Response Team (Colcert), and the Ministry of Foreign Affairs led a technical workshop aimed at raising awareness among digital service providers about the Second Additional Protocol to the Budapest Convention. The meeting, which was supported by the European Union's GLACY-e project (Global Action on Cybercrime Enhanced) and the Council of Europe, seeks to prepare the country for the potential ratification of this legal instrument, designed to expedite the cross-border collection of electronic evidence in criminal investigations.

COLOMBIA AND MEXICO CONSOLIDATE ALLIANCE TO STRENGTHEN REGULATORY COOPERATION IN COMMUNICATIONS

trendTIC – The Communications Regulatory Commission (CRC) and the Telecommunications Regulatory Commission (CRT) are strengthening their technical and regulatory cooperation within a collaborative framework that seeks to promote the exchange of experiences and contribute to the joint analysis of the challenges of the digital ecosystem, fostering the development of more efficient, competitive, and innovative markets. The Memorandum establishes a non-binding framework for collaboration, within the purview of each entity, focused on the exchange of technical knowledge and best regulatory practices. Its objective is to contribute to the analysis and addressing of current and future challenges in the telecommunications, broadcasting, and digital services sectors, in a context of rapid technological transformation.

COMMANDERS FROM ACROSS THE CONTINENT DISCUSS ORGANIZED CRIME AND CYBERSECURITY

Ultima Hora - The Conference of American Armies, being held in Asunción until Friday, the 27th, opened on Tuesday with the presence of President Santiago Peña. The conference aims to analyze the "multidimensional challenges to the defense and strategic security of the member countries." The Commander of the Paraguayan Army and President of the Conference of American Armies, General Manuel Rodríguez Sosa, delivered the opening remarks at the inaugural session.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 26, 2026

THE BIGGEST DIGITAL CHALLENGE OF THE 2026 WORLD CUP: UNPRECEDENTED CYBERATTACKS, BETTING, AND TRAFFIC

Pulzo - With the FIFA World Cup approaching in June 2026, it's not just the stadiums and teams that will be under pressure; the global digital landscape will also face one of its greatest challenges. This sporting event, considered the most-watched on the planet, triggers a massive concentration of online activity across sectors as diverse as digital betting, gaming, ticket sales, e-commerce, media, and social networks. The simultaneous interaction of millions of users—whether searching for information, sharing emotions, or placing bets—creates an unprecedented scenario of high demand on technological infrastructure.

ARTIFICIAL INTELLIGENCE ALLOWS CYBERATTACKS TO BE CARRIED OUT IN JUST 27 SECONDS

Infobae - The accelerated use of artificial intelligence (AI) by cybercriminal groups has led to sophisticated attacks being launched in just 27 seconds, a phenomenon that is radically transforming digital security globally. According to the Global Threat Report 2026 published by CrowdStrike, the combination of AI innovations and attackers' instant adaptation is drastically reducing response times and increasing the volume of threats against corporate infrastructure, presenting security professionals with an unprecedented scenario.

CHINA-LINKED HACKERS BREACHED DOZENS OF TELECOMS, GOVERNMENT AGENCIES

Cybersecurity Dive - Hackers working for the Chinese government broke into more than 50 telecommunications companies and government agencies in 42 countries, in a campaign that exploited cloud platforms’ legitimate features to hide the attackers’ tracks. “The attacker was using API calls to communicate with [software-as-a-service] apps as command-and-control (C2) infrastructure to disguise their malicious traffic as benign,” researchers at Google’s Threat Intelligence Group and Mandiant said in a report on Wednesday. Google said the “prolific, elusive” China-linked hacker team, which it tracks as UNC2814, “has a long history of targeting international governments and global telecommunications organizations across Africa, Asia, and the Americas.”

GENAI MISUSE & RANSOMWARE DRIVE SURGE IN CYBER ATTACKS

ITBrief - Organisations worldwide faced an average of 2,090 cyber attacks per week in January 2026, as ransomware activity increased and broader use of generative AI tools raised the risk of data exposure, according to new research from Check Point Research. The figure was up 3% from December and 17% year on year. Check Point attributed the rise to more frequent ransomware campaigns and gaps in governance around GenAI use on corporate networks. "January's data shows that cyber attacks are not only increasing but becoming more refined and opportunistic," said Omer Dembinsky, data research manager at Check Point Research. "Ransomware operators are accelerating their campaigns while unchecked GenAI usage is opening new blind spots for organizations. Prevention-first, real-time protection powered by AI is the only effective way to stop attacks before they cause operational or financial damage."