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 GOVERNMENT APPROVED THE FEDERAL PLAN TO COMBAT CYBER-ASSISTED FRAUD - ARGENTINA

The Truth - The Government, through the Ministry of Security, created the Federal Plan to Combat Cyber-Assisted Fraud, which seeks to strengthen prevention and detection efforts against cybercrime threats. The measure was announced this Monday in the Official Gazette. Resolution 231/2026, issued by the Ministry of Security, instructs the Directorate of Cybercrime and Cyber Affairs, under the Cabinet of Advisors, to "coordinate and carry out the necessary actions to achieve the comprehensive implementation" of the plan.

PUBLIC-PRIVATE SYNERGY FOR CYBERSECURITY AND DIGITAL TRANSFORMATION - MEXICO

Yahoo! News - Mexico's digital transformation is accelerating and demands increasingly close coordination between the government, the financial sector, and technology players. In this context, an institutional dialogue was recently held between Mexican financial institutions and the Digital Transformation and Telecommunications Agency, providing a forum to analyze some of the technology projects that will shape the future of the country's digital and financial ecosystem.

BRAZILIAN DIGITAL ECA COMES INTO EFFECT: WHAT THE LAW SAYS THAT SEEKS TO PROTECT MINORS ON THE INTERNET - BRAZIL

See - Starting this Tuesday, the 17th, the new rules of the Statute of Children and Adolescents (ECA Digital) regarding the protection of minors on the internet are in effect. The text creates a series of obligations to be fulfilled by social networks, streaming platforms, messaging applications, online games, adult websites, and other digital service providers operating in Brazil. According to the law, digital service providers become legally responsible for protecting children and adolescents from virtual threats and restricting their access to inappropriate content on the web.

MINISTRY OF MANAGEMENT AND CPQD ANNOUNCE ARTIFICIAL INTELLIGENCE PROJECT FOCUSED ON PERSONALIZED DIGITAL GOVERNMENT - BRAZIL

gov.br - a digital government for every person. With this focus, the Ministry of Management and Innovation in Public Services (MGI), in partnership with the Center for Research and Development in Telecommunications (CPQD), is initiating the development of an innovative project aimed at the digital transformation of the Brazilian State: INSPIRE - Artificial Intelligence in Public Service with Innovation, Responsibility and Ethics. The project was formalized this Tuesday (September 30th) in Campinas. A total investment of R$ 390 million is planned over the period. The four-year project is the result of a commission from the National Fund for Scientific and Technological Development (FNDCT), administered by the Ministry of Science, Technology and Innovation (MCTI), and managed by the Financing Agency for Studies and Projects (Finep).

THE BRAZILIAN ARMY IS PREPARING FOR THE LARGEST CYBER DEFENSE EXERCISE IN THE SOUTHERN HEMISPHERE

Defense Net - The Brazilian Army, through the Cyber Defense Command (ComDCiber), as part of the preparation activities for Exercise Cyber Guardian 8.0 (EGC 8.0), conducted a technical visit to the Amazon Military Command (CMA) from March 2nd to 5th. During the visit, the ComDCiber delegation presented aspects of the exercise planning to the CMA and representatives from the Government and the State University of Amazonas (UEA), as well as the possibilities for participation by companies and academia in the constructive and virtual simulation activities of EGC 8.0.

CYBER THREATS: HOW THE GSI ASSESSES THE RISKS OF TECHNOLOGY TO STATE SECURITY - BRAZIL

Veja magazine reports that increasingly sophisticated and accessible artificial intelligence, along with its rampant development, brings a wide range of threats to the stability of institutions and the integrity of information in public debate. One imminent challenge is the flood of "deepfakes" of politicians on social media, which is challenging the control mechanisms of the Electoral Court. In parallel to the work of the Justice system, the effort to assimilate new technologies and combat threats to national stability is one of the responsibilities of the Institutional Security Office (GSI), a federal government body directly responsible for assessing risks to institutions and the democratic rule of law.

THE CYBERSECURITY INDUSTRY IS GROWING "UNPRECEDENTEDLY" IN SPAIN AND IS DEMANDING MORE PROFESSIONALS

Telepress - The director of the National Cybersecurity Institute (Incibe), Félix Barrio, highlighted this Wednesday the "unprecedented" growth of the cybersecurity industry, a "vital" sector of the economy for the functioning of society and the economy, with 3,430 companies representing one of the "most vibrant" technology markets in Europe, whose main challenge is the training of professionals. In this regard, he specified that in just four years the sector, which employs 162,000 workers, has grown by 35 percent in terms of employment and has led to the implementation of 403 entrepreneurial projects.

DIGI AMERICAS LATAM CISO

INSIGHTS

MARCH 19, 2026

HOW SHOULD EDUCATIONAL INSTITUTIONS PREPARE FOR THE INCREASE IN CYBERATTACKS?

E&N - With the start of the academic year in the region, experts are warning of the urgent need to strengthen digital security in schools and universities, given the sustained increase in cyberattacks targeting the education sector. Digital threats no longer discriminate based on industry or organizational size. Cybercriminals have sophisticated their tactics, combining ransomware, data extortion, and vulnerabilities associated with the use of Generative Artificial Intelligence (GenAI) tools.

DOE'S CESER STRATEGIC PLAN SETS THREE-PRONGED STRATEGY TO HARDEN ENERGY INFRASTRUCTURE, BOOST CYBER RESILIENCE - USA

Industrial Cyber - The U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response published its first five-year strategic plan for fiscal years 2026 to 2030, outlining a roadmap to strengthen the security and resilience of the U.S. energy sector. With three goals, the 'CESER Strategic Plan Fiscal Years 2026 to 2030' plan emphasizes priorities such as advancing American energy dominance and hardening critical infrastructure against an increasingly complex and evolving threat landscape, while reaffirming CESER's core mission to protect and secure the nation's energy systems.

HOW DIGITAL SYSTEMS COULD STABILIZE A FRACTURED VENEZUELA

Duke Cybersecurity Hub - Venezuela's crisis is often described in terms of ideology, sanctions, or political stalemate. Yet beneath these visible pressures lies a deeper problem: the collapse of the basic systems that sustain a modern society. Without trusted mechanisms for identity, payments, records, and accountability, no political or economic recovery can be sustained. Rebuilding Venezuela will therefore require more than elections or macroeconomic adjustments. It will require restoring the digital foundations of trust that underpin governance, markets, and social cohesion, drawing on lessons from other fragile and transitioning states.

INTERPOL REPORT WARNS OF INCREASINGLY SOPHISTICATED GLOBAL FINANCIAL FRAUD THREAT

Interpol - Financial fraud is now one of the world's most severe and rapidly evolving transnational crimes, with significant economic and human consequences. The 2026 INTERPOL Global Financial Fraud Threat Assessment warns that with increased global criminal collaboration, fraud is no longer a peripheral threat, it is at the centre of polycriminality, intersecting with organized crime, human trafficking and cybercrime.

MASTERCARD SURVEY REVEALS NEW CONCERNS AMONG CONSUMERS IN LATIN AMERICA AND THE CARIBBEAN

WJournal - Mastercard presented the results of its latest regional survey focused on cybersecurity perceptions in Latin America and the Caribbean. The study revealed that, as digital payments become more integrated into daily life and convenience increases, a new paradigm is emerging in the region: although consumers feel increasingly confident in their ability to navigate the digital world, the fear of fraud and scams remains their biggest concern.