



INSIGHTS

OCTOBER 9, 2025

DIGI AMERICAS ALLIANCE MEMBERS



PROJECT SETS ASIDE MONEY FROM BETTING TO COMBAT DIGITAL CRIMES - BRAZIL

Brazilian Senate - The Senate is analyzing a bill that creates a legal framework for cybersecurity and allocates more resources for the National Public Security Fund (FNPS) to use in combating digital crimes. Bill 4,752/2025 was proposed by Senator Esperidião Amin (PP-SC) and is currently under review by the Constitution and Justice Committee (CCJ). Bill 4,752/2025 creates the National Digital Security and Resilience Program. Linked to the federal government, the plan may count on the support of states, the Federal District, municipalities, and private sector organizations. The program's objectives include: improving the investigation and combat of cybercrime; establishing national, state, district, and municipal cyber resilience plans; and integrating actions across critical sectors such as healthcare, education, finance, energy, telecommunications, transportation, the environment, defense, and public safety.

GSI/PR PUBLISHES STANDARD FOR THE USE OF CLOUD COMPUTING FOR PROCESSING CLASSIFIED INFORMATION - BRAZIL

GSI - Institutional Security Office of the Presidency of the Republic (GSI/PR) published this Tuesday (7) a Normative Instruction that regulates the treatment of classified information in cloud computing environments within the Federal Public Administration. The standard represents a milestone in the modernization of information security standards, by allowing, under strict security, control and audit conditions, the use of advanced technological solutions compatible with the most demanding international parameters.

DATA GOVERNANCE: AN ESSENTIAL REQUIREMENT FOR IMPLEMENTING THE NEW DATA PROTECTION LAW - CHILE

TrendTIC - The entry into force of Law 21,719 on Personal Data Protection marked a milestone in Chile. It established, for the first time, the implementation of a Breach Prevention Model (BPM), a compliance program under which a series of procedures and obligations are adopted regarding personal data, allowing companies to demonstrate due diligence and mitigate penalties.

DIGI
AMERICAS



INSIGHTS

OCTOBER 9, 2025

THE COUNTRY'S DEFENSE IS ALSO FOUGHT IN CYBERSPACE: SSPC - MEXICO

OEM - Every secure password, every antivirus update, every suspicious link we choose not to open are small actions that build a collective wall of security, said Israel Agüero Alegría, Director General of Cybersecurity and Technological Development at the Secretariat of Security and Citizen Protection (SSPC). Participating in the inauguration of the Tenth National Cybersecurity Week, organized by the National Guard, the official said that the first line of defense lies not in technology specialists or systems managers, but in the responsibility of individuals, of users of social networks and digital services.

SHEINBAUM SEEKS TO EXPAND NAVY POWERS: HIGH-SEAS PURSUIT, CYBERSECURITY, AND ARTIFICIAL INTELLIGENCE - MEXICO

Segundo a Segundo - President Claudia Sheinbaum sent to the Chamber of Deputies a reform initiative to the Organic Law of the Mexican Navy. This initiative proposes expanding the naval institution's responsibilities with new powers in high-seas pursuit, cybersecurity, and the use of artificial intelligence in scenarios that affect national security. It would also be given cyberdefense and cybersecurity tasks, allowing it to operate in cyberspace alongside other authorities, as well as powers to exercise naval control of maritime traffic and protect it in Mexican maritime zones and corresponding airspace.

GEO AI: THE CONFLUENCE OF ARTIFICIAL INTELLIGENCE AND GEOGRAPHY THAT IS TRANSFORMING COLOMBIA

ImpactoTIC - The ESRI 2025 User Conference, held at the Bogotá Agora and attended by more than 2,600 participants, established itself as the most important geospatial technology event in the country. This year's central theme was the convergence between Artificial Intelligence (AI) and Geographic Information Systems (GIS), a concept ESRI is promoting as GEO AI or Geospatial Intelligence.

NATO: "WE ARE PREPARING AS BEST WE CAN FOR THIS HYBRID WAR OF THE FUTURE."

Yahoo! News - NATO members, especially in Europe, face hybrid attacks: cyberattacks, disinformation campaigns, drone harassment. Modern guerrilla warfare is waged online and in the air, using low-cost resources that easily fall into the hands of attackers. The goal is to disrupt everyday life and damage the morale of European citizens. Manfred Boudreaux-Dehmer, NATO's first Chief Information Officer (CIO), estimates that such attacks are likely to become increasingly frequent in the future.

DIGI
AMERICAS



INSIGHTS

OCTOBER 9, 2025

CRIMINAL AI, THE NEW GLOBAL DIGITAL THREAT

America Retail - Criminal AI, the new global digital threat, artificial intelligence (AI) has transformed the business world, but it has also taken a disturbing turn in the field of cybercrime. According to the semi-annual report by Trend Micro, a global leader in cybersecurity, more than 60% of the world's population could be affected by AI-driven digital attacks by 2025. This new reality places governments, businesses, and users facing an unprecedented threat, where the automation and precision of artificial intelligence are being used for criminal purposes.

PHYSICS NOBEL AWARDED TO THREE SCIENTISTS FOR WORK ON QUANTUM COMPUTING

BBC - The Nobel Prize in Physics has been awarded to John Clarke, Michel H. Devoret and John M. Martinis for their work on quantum mechanics that is paving the way for a new generation of very powerful computers. "There is no advanced technology used today that does not rely on quantum mechanics, including mobile phones, cameras... and fibre optic cables," said the Nobel committee.

WHY CYBERSECURITY'S FUTURE DEPENDS ON PEOPLE, NOT JUST TECHNOLOGY

WEF - For years, the story of cybersecurity has been told in the language of machines. Firewalls, antivirus software, intrusion detection systems and now quantum computing and artificial intelligence — each new tool promised to outpace the next wave of attackers. But for all of this innovation, breaches still happen every day and most of them are not caused by cutting-edge exploits, but by people. In 2024, for example, 95% of data breaches were tied to human error.

SIGNAL INTRODUCES NEW POST-QUANTUM CRYPTOGRAPHIC DEFENSE TO SECURE MESSAGING AGAINST FUTURE QUANTUM THREATS

The Cyber Security Hub - Signal, the widely used encrypted messaging platform, has unveiled a major step forward in safeguarding communications against the looming threat of quantum computing. The non-profit Signal Foundation announced the deployment of Sparse Post-Quantum Ratchet (SPQR), a new cryptographic system designed to ensure long-term privacy in a world where quantum computers may render traditional encryption obsolete.

WHY CYBER RESILIENCE IN SPACE IS ESSENTIAL FOR ECONOMIC SECURITY

WEF - From international finance and climate monitoring to navigation and humanitarian assistance, satellite services from space are now woven into the fabric of modern life. Valued at over \$630 billion in 2023, with projections exceeding \$1.8 trillion by 2035, space has shifted from frontier to foundational infrastructure. Yet as space becomes indispensable, it is increasingly contested. Cyber disruptions, jamming attacks and geopolitical manoeuvres highlight a fragility that coexists with rapid innovation.