



INSIGHTS

MAY 8, 2025

DIGI AMERICAS ALLIANCE MEMBERS



BANCO DO BRASIL DEFINES GUIDELINES FOR THE USE OF AI

Digital Convergence - The growing use of artificial intelligence by employees is bringing new security concerns to the banking sector. Marco Antonio Mantovani, information security manager at Banco do Brasil, highlights that, although AI brings benefits, it is crucial to ensure the protection of corporate and customer data. "Today, all companies are using AI to integrate business. In the banking sector, we first observed its use in chats, chat bots, WhatsApp, in various channels, and in virtual assistants as well. And in models. We have models for credit, risk, purchases, process automation, and more recently coding. A very important factor in AI is that people, employees, have also realized the advantage of using it in their daily lives and want to use AI for the activities they perform. So, in addition to having a team to create AI for business, we also have to disseminate this so that our employees can use it safely," says Mantovani.

CHICO RODRIGUES DEFENDS NATIONAL CYBERSECURITY PLAN - BRAZIL

Senado - In a speech in the Plenary on Tuesday (6), Senator Chico Rodrigues (PSB-RR) highlighted an official trip he made to the United States to participate in the RSA Security Conference, one of the main global events on information security. According to him, the delegation also included the participation of Senators Esperidião Amin (PP-SC), Marcos Pontes (PL-SP), Jorge Seif (PL-SC) and Sergio Moro (União-PR).

Source: Senate Agency

THE DOMINICAN REPUBLIC AND THE UNITED ARAB EMIRATES SIGN A COOPERATION AGREEMENT TO STRENGTHEN CYBERSECURITY.

Presidency - The Dominican Republic and the Government of the United Arab Emirates signed a cooperation agreement in Dubai to strengthen cybersecurity in the country, within the framework of the GISEC Global 2025 event. The signing ceremony was carried out by the highest authorities of the governing bodies of cybersecurity of both governments: the National Cybersecurity Center, an entity attached to the National Department of Investigations (DNI), its director, Mr. Luis Soto, and the Cybersecurity Council of the United Arab Emirates, its director, Dr. Mohamed Al-Kuwaiti.

DOMINICAN REPUBLIC LEADS REGIONAL DIALOGUE ON CYBERSECURITY IN CIVIL AVIATION

El nuevo Diario - The Dominican Republic is hosting the Thirteenth Meeting of the Regional Group on Cybersecurity in Aviation and Conflict Zones, an important gathering organized by the International Civil Aviation Organization (ICAO) that brings together delegations from North America, Central America, the Caribbean, and South America. The meeting, held from May 5 to 9 at a hotel in the capital, is coordinated by the Specialized Corps on Airport and Civil Aviation Security (CESAC), reaffirming the country's commitment to strengthening regional air security. This international meeting is part of the security policies promoted by President Luis Abinader and the Ministry of Defense, reflecting the Dominican State's commitment to complying with international standards in civil aviation and cybersecurity.

\$12 MILLION BUDGET APPROVED FOR THE CYBERSECURITY AGENCY - EL SALVADOR

Prensa Grafica - A total of \$12 million is the amount that the Legislative Assembly approved for the State Cybersecurity Agency (ACE) to carry out its functions through 2025. So far, the officials who will be in charge of the institution are unknown. According to the decree, the Ministry of Finance determined the special budget for the agency to begin operating from April to December of this year. The amount will be incorporated into the General State Budget for the Justice and Public Security branch, to which the ACE is attached. The funds will be transferred from the Ministry of Finance's allocations. However, the approved initiative did not explain which budget unit would be cut to make the transfer, and no ruling party representative asked or commented on the matter.

CFE INVESTS MORE THAN 400 MILLION PESOS IN CYBERSECURITY AFTER GLOBAL BLACKOUTS - MEXICO

infobae - The Federal Electricity Commission (CFE) announced an investment of more than 400 million pesos in cybersecurity strategies and technologies in response to the growing risk of cyberattacks threatening energy infrastructure worldwide. This decision comes after a series of global blackouts and cyberattacks that have highlighted the vulnerability of interconnected electrical systems. According to the company, the allocated budget will focus on modernizing systems, strengthening data protection protocols, hiring cybersecurity experts, and acquiring advanced technology for real-time threat monitoring and detection.

DIGITAL GOVERNANCE IN THE DEFENSE SECTOR: AN URGENT CHALLENGE - COLOMBIA

CGFM - Innovation plays a crucial role in the evolution of digital governance in the defense and security sector. The Innovation Force Hub plays a strategic role. Cyber threats are growing and require more coordinated responses. Cyberattacks on strategic infrastructure such as military radars, communications systems, and data networks in the Defense Sector have become growing threats to national security. To respond to these vulnerabilities, the Ministry of Defense is designing the Innovation Force Hub in collaboration with academia, the private sector, the State, and civil society to foster the adoption of advanced technological solutions.

THE WATER SECTOR MUST ALSO PROTECT ITSELF AGAINST CYBERATTACKS

The conversation - Digitalization undoubtedly represents an essential advancement in all sectors, including water. However, digital advances also bring new threats and, therefore, growing concerns about cybersecurity. As evidence of this, the European Union's NIS2 Directive 2022/2555 covers both drinking water and wastewater and stipulates various obligations regarding cybersecurity management for the sector.

IBERIAN BLACKOUT: CYBERATTACK IS NOT TO BLAME - BUT THE THREAT TO POWER GRIDS IS REAL. HERE'S WHY

WEF - Millions of people across Spain and Portugal experienced a major power outage on Monday, causing significant travel disruptions and bringing much of the economy to a standstill. The sudden blackout led many private and public sector experts, including top government officials, to question whether the disruption could have been caused by a cyberattack. Spain's top criminal court, for instance, quickly announced that it was probing the possibility of an "act of cyber sabotage against critical Spanish infrastructure."

U.S. QUANTUM INDUSTRY LEADERS PRESS CONGRESS TO EXPAND U.S. SUPPORT

The Quantum Insider - Although reports on the Trump administration's "skinny budget" dashed hopes for a revived National Quantum Initiative, politicians and quantum experts added weight to the proposed reauthorization in testimony before the House Science Committee. During a May 7 hearing, members of the Congressional committee and executives from leading quantum companies called for increased federal support to keep the United States competitive in a fast-moving global quantum race. The original National Quantum Initiative Act, passed in 2018, elevated quantum information science as a national priority, leading to the creation of research hubs, the formation of a public-private consortium and a more coordinated approach to quantum development across federal agencies.