



INSIGHTS

APRIL 24, 2025

DIGI AMERICAS ALLIANCE MEMBERS



DOMINICAN REPUBLIC | SIGNS AGREEMENT WITH COSTA RICA TO ADVANCE SECURE DIGITAL TRANSFORMATION

dplnews - During a live virtual event, the Dominican Republic and Costa Rica signed a cooperation agreement on digital transformation and cybersecurity, with an emphasis on the mutual recognition of digital signatures. This agreement aims to promote secure, interoperable technologies focused on citizen well-being. The initiative was signed by Guido Gómez Mazara, president of the Dominican Telecommunications Institute (Indotel), and Paula Bogantes Zamora, Minister of Science, Innovation, Technology and Telecommunications (MICITT) of Costa Rica, who highlighted the importance of this agreement in strengthening bilateral relations.

ANALYSIS OF CYBERSECURITY LAW INITIATIVE ADVANCES - GUATEMALA

Congreso.gob.gt - To continue the analysis and discussion of Initiative 6347, the cybersecurity law, the National Security Affairs Committee, chaired by Representative Jorge Mario Villagrán, held a hybrid meeting this Wednesday. On this occasion, the representatives who make up the Legislative Chamber defined a package of 11 sanctions and prison sentences for cybercrimes, corresponding to the second title of the aforementioned initiative. During the meeting, the parliamentarians reviewed the prison sentences and sanctions currently stipulated in the Penal Code, Decree 17-73, and the Code of Criminal Procedure, Decree 51-92. Based on a comparative table, they defined the increases in prison sentences, sanctions, and fines that must be approved to prevent and eradicate cybercrimes in accordance with international and national regulations.

CHALLENGES AND KEY ASPECTS OF NEW CYBERSECURITY AND DATA PROTECTION LAWS IN EL SALVADOR

E&N - With the entry into force of the Cybersecurity and Information Security Law, the Personal Data Protection Law, and the new technical standards of the Central Reserve Bank (NRP-23 and NRP-24), Salvadoran organizations face a new regulatory landscape. To comply with these provisions, companies must make profound legal and technical adjustments, implement solid governance structures, and adopt an organizational culture focused on digital security.

NEARSHORING AND CYBERSECURITY - MEXICO

Aristegui - Despite the current complex economic climate, the growth of nearshoring is playing a significant role in the evolution of industrial cybersecurity in Mexico. Global companies have invested in the country, bringing with them high security standards, encouraging local companies to modernize.

Today, Mexico ranks 7th worldwide in cyberattacks, and the manufacturing sector has responded with innovation and unity, as companies understand that a cyberattack can not only generate economic losses but also human risks at critical facilities.

THE GOVERNMENT PROMOTES CYBERSECURITY TRAINING FOR MORE THAN 6,000 CIVIL GUARD OFFICERS - SPAIN

infobae - The Ministers of the Interior and Digital Transformation and Public Service, Fernando Grande-Marlaska and Óscar López, respectively, signed a declaration of intent this Monday to promote cybersecurity training for Civil Guard professionals. According to the Ministry of the Interior in a press release, the initiative is aimed at more than 6,000 Civil Guards who will be able to benefit from this distance learning provided by the National Cybersecurity Institute (INCIBE) in collaboration with the UNED (National University of Education).

FOR THE FIRST TIME, NVIDIA CHIPS AND SUPERCOMPUTERS WILL BE MANUFACTURED IN THE UNITED STATES

dplnews - Nvidia is collaborating with its manufacturing partners, TSMC and Foxconn, to design and build factories that will, for the first time, produce Nvidia's artificial intelligence (AI) supercomputers entirely in the United States. Together with TSMC, Nvidia has launched more than 1 million square feet of manufacturing space to build and test Blackwell chips in Arizona; while with Foxconn, it is building AI supercomputer manufacturing plants in Texas.

FINANCIAL SECTOR STRENGTHENS ITS DIGITAL DEFENSE: INVESTMENT IN CYBERSECURITY GREW 16%

Portafolio - Last year, the digital landscape was characterized by accelerated technological adoption and a cross-cutting digital transformation in strategic sectors such as finance, manufacturing, healthcare, energy, transportation, and public administration. This scenario drove significant advances in cybersecurity and information protection throughout Latin America.

80% OF CYBERSECURITY MANAGERS WILL SEE THEIR JOBS ENHANCED BY GENERATIVE AI

Business Empresarial - A recent CrowdStrike study indicates that 76% of security leaders in organizations are looking for generative AI solutions specifically geared toward cybersecurity, highlighting the importance of integrating these tools to improve threat detection. The analysis, titled State of AI in Cybersecurity 2024, shows that 80% of decision-makers are choosing generative AI within unified platforms, rather than isolated tools. Furthermore, a similar proportion of professionals prefer solutions specifically designed to improve security rather than general-purpose applications.

CYBERSECURITY INVESTMENTS, A GROWING PRIORITY FOR LATIN AMERICAN COMPANIES

America Retail - Investments in Cybersecurity, a Growing Priority for Latin American Companies. As Latin America moves toward a digital era, cybersecurity has become a major concern for companies in the region. With the increased use of emerging technologies, especially artificial intelligence (AI), in both the public and private sectors, the risks associated with cyberattacks have also grown. In this context, Latin American companies are redoubling efforts to protect their systems and data against digital incidents, a challenge that has taken on greater relevance due to new cybersecurity legislation and the growing sophistication of cybercriminals.

U.S. RECIPROCAL TRADE POLICY: STRATEGIC OPPORTUNITIES FOR LATIN AMERICA AMID GLOBAL UNCERTAINTY

CSIS - The adoption of a reciprocal trade policy by the United States represents one of the most significant shifts in the country's economic approach in decades. As businesses and investors respond to this evolving landscape, both unprecedented opportunities and substantial risks emerge. The strategic recalibration of U.S. trade posture offers forward-thinking organizations a chance to address longstanding barriers while necessitating careful avoidance of potential disruptions in global supply chains and technology ecosystems.

THREE KEY WAYS TO MAKE SUPPLY CHAINS MORE RESILIENT TO CYBER RISKS

WEF - In a technologically dependent and interconnected society, managing cyber risk within global supply chains is critical. Misaligned market incentives, risk inequality and limited visibility across supply chains require new principles to boost ecosystem resilience. These three new principles should foster embeddedness, leverage advanced technology and be adaptive and proactive.

THE IMPACT OF AI REGULATIONS ON CYBERSECURITY STRATEGY

Cyber Security News - Artificial Intelligence (AI) is transforming the cybersecurity landscape, offering both powerful tools for defense and new avenues for attack. As organizations increasingly adopt AI-driven solutions to detect threats, automate responses, and analyze vast amounts of data, governments and regulatory bodies are racing to create frameworks that ensure the responsible use of these technologies.

CYBERCRIMINALS BLEND AI AND SOCIAL ENGINEERING TO BYPASS DETECTION

Help Net Security - Attackers are focusing more on stealing identities. Because of this, companies need to use zero trust principles. They should also verify user identities more carefully. Researchers analyzed thousands of alerts, mapping them to the MITRE ATT&CK framework, a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

AFRICA IN THE CROSSHAIRS AS ASIA'S CYBERCRIME RINGS GO GLOBAL

TechCentral - Asian crime syndicates behind the multibillion-dollar cyberscam industry are expanding globally including to Africa and South America, as raids in Southeast Asia fail to contain their activities, the United Nations said in a report on Monday. Criminal networks that emerged in Southeast Asia in recent years, opening sprawling compounds housing tens of thousands of workers, many trafficked and forced to scam victims around the world, have evolved into a sophisticated global industry, the United Nations Office on Drugs and Crime (UNODC) said.

CYBER-RISKS IN THE WATER SECTOR: MODERNISE AND SEGMENT TO PROTECT YOURSELF

Stormshield - A recent study by France's national Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) information systems security agency assessed the risks to which businesses and local authorities are exposed. At least 31 compromises affecting players in the water sector in France have been examined by ANSSI since 2021, warning of clear vulnerabilities in water and wastewater services. While efforts have already been made, organisations still need to strengthen their defensive stance, as befits the critical nature of their business.

THIS IS THE STATE OF PLAY IN THE GLOBAL DATA CENTRE GOLD RUSH

WEF - Data centres are proliferating rapidly, with demand driven by AI. They are not just digital infrastructure, but also high-value investment assets. Energy consumption, regulatory complexity and geopolitical tensions are potential obstacles to future growth in the sector.