INSIGHTS

MARCH 20, 2025

INTER-INSTITUTIONAL COMMISSION STRENGTHENS FIGHT AGAINST ELECTRONIC FRAUD IN COSTA RICA

elmundo.cr - An inter-institutional commission, coordinated by the Chamber of Banks and Financial Institutions, has implemented priority actions to combat electronic fraud and cybersecurity threats in Costa Rica. The commission includes the participation of the Central Bank of Costa Rica (BCCR), the General Superintendency of Financial Entities (SUGEF), the Public Prosecutor's Office (MP), and the Judicial Investigation Agency (OIJ).

REPRESENTATIVE NERY RODAS PRESENTS A BILL TO CREATE A DIGITAL TRANSFORMATION SUPERINTENDENCY - GUATEMALA

LaHora.gt - Cabal Party representative Nery Rodas presented the bill creating a digital transformation superintendency this Thursday, March 13, a project discussed during the parliamentary forum on digital transformation. The bill seeks to establish a legal framework for digital transformation and modernize digital services that lead to technological innovation. According to the bill, the institution to be established would be comprised of a board of directors, an advisory board, a superintendent, and mayors. The three state agencies, the National Association of Municipalities (ANAM) and the National Registry of Persons (RENAP), will be responsible for appointing officials to that entity.

GUATEMALA | THE MINISTRY OF EDUCATION PRESENTED ITS EDUCATIONAL TECHNOLOGY PLAN TO CONGRESS

dplnews - Education Minister Anabella Giracca appeared before Congress to explain how they would implement Bill 5891, on Universal Access to Educational Technology. This seeks to strengthen education in the country by incorporating technology into classrooms. According to the minister, this strategy would cover grades four, five, and six onward, with the goal of modernizing learning and improving student opportunities.

REGULATION OF VIRTUAL ASSET SERVICE PROVIDERS (VASPS) – ARGENTINA

Argentina.gob.ar - In compliance with the legal mandate established in Law No. 27,739, which designates the National Securities Commission (CNV) as the regulator of Virtual Asset Service Providers (VASPs), and following the public consultation carried out through RG No. 1025, the CNV approved General Resolution No. 1058, which establishes the regulations for VASPs. The resolution aims to guarantee transparency, stability, and user protection in the crypto ecosystem, imposing obligations regarding registration, cybersecurity, asset custody, money laundering prevention, and risk disclosure.

CYBERSECURITY AND NEW TECHNOLOGIES: THE BIGGEST CONCERNS OF ARGENTINE COMPANIES

Radiomaster - Cyber incidents have become the top risk for businesses in Argentina, surpassing other key factors such as inflation, natural disasters, legislative changes, climate change, and market developments. According to the Allianz Risk Barometer 2025, more than 60% of respondents globally identified data breaches as the most feared cyber exposure, followed by attacks on critical infrastructure and physical assets (57%).

MITIC TRAINS GOVERNMENT OFFICIALS IN CYBERSECURITY WITH SUPPORT FROM TAIWAN – PARAGUAY

Paraguayan Information Agency - The Ministry of Information and Communication Technologies (Mitic), through the Cyber Incident Response Center (CERT-PY), launched the "Cybersecurity Training for State Agencies and Entities" program. This program will be developed from March 14 to June 26, 2025, in a hybrid format through the Mitic Campus, the institution's virtual platform. The training program for state officials is supported by the Embassy of Taiwan in Paraguay and aims to strengthen cybersecurity capabilities by developing topics such as Incident Response, Threat Intelligence Gathering, Penetration Testing, Cybersecurity Diagnostics, Digital Forensics, and Investigation.

NEW MEASURES TO COMBAT DIGITAL BANKING FRAUD IN BRAZIL ANNOUNCED

E.M. Foco - Recently, the Ministry of Justice and Public Security, in partnership with the Brazilian Federation of Banks (Febraban), announced a new national alliance with the aim of combating digital banking fraud. This initiative seeks to implement effective measures to prevent online scams and improve victim support. The joint effort involves the collaboration of banks, telephone companies, online commerce and social networks, aiming to develop robust security measures.

AIG ADDRESSES CYBERSECURITY INCIDENTS THROUGH CSIRT PANAMA

telemetro.com - The National Authority for Government Innovation (AIG) announced that, starting with this communication, all cybersecurity incident reports in government entities will be handled exclusively by the Panama Cybersecurity Incident Response Team (CSIRT PANAMA). To ensure efficient and timely response, the AIG has enabled the email address incidencias@cert.pa as the sole official channel for receiving and managing these reports.

URUGUAY IS INVESTIGATING A CYBERATTACK ON AN OFFICIAL WEBSITE ALLEGEDLY FROM ARGENTINA

Pagina12 - The Uruguayan government reported this Monday that it is investigating a cyberattack on official websites, allegedly carried out from Argentina, which exposed personal information of Uruguayan President Yamandú Orsi, including one of his phone numbers, and threatened other leaders and officials. Specifically, local media reported that a group of right-wing hackers attacked the official website of the National Directorate of Civil Aviation and Aeronautical Infrastructure (Dinacia). From there, the cyberattackers stated that "Uruguay is getting worse and worse" and that they were tired of "progressivism" and "the lies of politicians," among other messages.

ARTIFICIAL INTELLIGENCE IN SECURITY AND DEFENSE: ALLY OR RISK FOR URUGUAY?

Dialogo Americas - What happens to your data as you walk through the city? Cameras and sensors analyze your movements, record patterns and can even predict behavior. All thanks to artificial intelligence (AI). This technology is already part of our daily lives and, although it can make us feel safer, it also raises concerns about our privacy and the ethical boundaries we must establish. Is Uruguay prepared for this challenge? AI can help prevent crime, detect cyber threats and optimize military resources. But what happens if that technology is based on biased data? What if it becomes a tool for mass surveillance? The risks are not minor: loss of privacy, discrimination and failures that could endanger human lives.

CYBERSECURITY AND GENDER EQUALITY: HOW INSURERS CAN LEAD THE WAY IN DIGITAL PROTECTION FOR WOMEN

100seguro - In today's digital age, cybersecurity has become a priority for all sectors, including insurance. However, it is crucial that cybersecurity strategies are not one-size-fits-all, but rather consider the specific needs of different groups, especially women. Insurers have an opportunity to innovate in this area, developing solutions that protect women against threats such as digital harassment and identity theft, thus fostering a more inclusive and secure digital environment.

MEDUSA RANSOMWARE SLAMS CRITICAL INFRASTRUCTURE ORGANIZATIONS

CybersecurityDive - The Medusa ransomware gang has infected more than 300 organizations in critical infrastructure sectors such as the medical, manufacturing and technology industries.
That's according to a joint cybersecurity advisory published Wednesday by CISA, the FBI and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The agencies noted that Medusa — which is not connected to MedusaLocker ransomware — has been active since 2021 and initially began as a closed ransomware operation.

THE ROLE OF LOCALIZATION IN CYBERSECURITY THREAT MITIGATION

Tripwire - If your website is targeting multiple states or countries, by default, you face a double-pronged challenge: adapting to regional regulatory demands while defending against sophisticated cyber threats. Tackling this requires localization. But what does the term actually entail?Localization isn't just about tailoring products, services, and infrastructure to meet local market requirements; it has emerged as a critical tool for compliance and cybersecurity threat mitigation. Strategic localization can address supply chain vulnerabilities, enhance regional threat intelligence, and foster resilience in a fragmented cyber ecosystem.

SECURITY OPERATION CENTER AS A SERVICE MARKET IS PREDICTED TO REACH USD 15.0 BILLION AT A CAGR OF 10.58% BY 2035

Einpresswire - The Security Operation Center as a Service (SOCaaS) market is projected to expand from USD 4.96 billion in 2024 to USD 15.0 billion by 2035, with an anticipated CAGR of approximately 10.58% during the forecast period from 2025 to 2035. The Security Operation Center as a Service (SOCaaS) market is experiencing significant growth as organizations increasingly prioritize cybersecurity in response to evolving digital threats. SOCaaS provides businesses with outsourced security operations, offering real-time threat monitoring, incident response, and risk management without requiring extensive in-house resources. The demand for SOCaaS is driven by the rising frequency of cyberattacks, stringent regulatory compliance requirements, and the growing adoption of cloud-based services.