aws | Apple | CHECK POINT | CISCO | CLOUDFLARE | CROWDSTRIKE | fluid attacks we hack your software | Google | GRUPO RADICAL | LUMU

mastercard | METABASE Q | netskope | paloalto NETWORKS | Santander | Schneider Electric | SISAP Sistemas Aplicativos | Telefónica | tenable | Trellix

TREND

COLOMBIA STRENGTHENS ITS DIGITAL SECURITY AND SPACE AFFAIRS WITH THE SIGNING OF SIX ALLIANCES AT ANDICOM 2024

Presidency - Within the framework of Andicom 2024, the main congress on information and communication technologies in Colombia, the country took a significant step towards strengthening its digital security and space issues by signing six memoranda of understanding with various strategic actors. Through the Digital Transformation team, led by Saúl Kattan Cohen, the Presidency of the Republic signed these alliances with six leading companies in the technology sector, to enhance the protection of critical infrastructures, promote international cooperation and strengthen the skills of Colombians in space issues and cybersecurity, in line with the government's digital transformation objectives.

COLOMBIA AND JAPAN SIGN MEMORANDUM TO STRENGTHEN INFORMATION TECHNOLOGY IN THE COUNTRY

Presidency - Within the framework of Andicom 2024, the ICT Ministry of Colombia and the Ministry of Internal Affairs and Communications of Japan signed a Memorandum of Cooperation to promote the development of Information and Communications Technologies (ICT) in both countries. The agreement, signed by the ICT Minister, Mauricio Lizcano, and the Japanese Vice Minister, Takuo Imagawa, seeks to improve connectivity, cybersecurity and the use of artificial intelligence, with a focus on sustainable development and social well-being.

PROSECUTORS ANNOUNCE OPENING OF INVESTIGATION INTO ACQUISITION OF PEGASUS SOFTWARE – COLOMBIA

Congress Magazine - The Attorney General's Office seeks to determine responsibilities for illegal use of Pegasus software. The control entity announced the opening of an investigation to determine those responsible, following the complaint by President Gustavo Petro regarding the acquisition of Pegasus spy software during the government of Iván Duque. According to the president, $11 million would have been delivered with authorization from the Police Intelligence Directorate (DIPOL), for the purchase of this Israeli software.

WHO IS RESPONSIBLE FOR THE COPPEL HACK THAT LASTED 3 MONTHS? – MEXICO

Correo Newspaper - In April 2024, the Lockbit 3.0 cybercriminal group, one of the most dangerous groups in the world in the field of ransomware, carried out a devastating attack against Tiendas Coppel. The hack limited at least 9,500 of the company's business services for three months and affected the operations of its 1,800 stores across the country. Lockbit 3.0, known for its ability to spread and renew ransomware, exploited a gap in Coppel's cybersecurity to execute the attack.

LEARN MORE ABOUT THE INSURANCE AND CYBERSECURITY WORKING GROUP – BRAZIL

Gov.br - The Superintendence of Private Insurance (Susep) published yesterday (28) Ordinance 8,323, which establishes a Working Group (WG), of an advisory nature, with the purpose of discussing and preparing technical studies on the cybersecurity of the sector supervised by the Agency and the challenges and opportunities that the development of the digital economy brings to the Brazilian insurance sector. The WG will be composed of two subgroups that will have as reference the following thematic axes: I - New Insurance for the Digital Economy: beyond cyber risk; and II - Adaptation of the cybersecurity system of the supervised market to the National Cybersecurity Policy.

SUSEP LAUNCHES WORKING GROUPS TO DISCUSS REINSURANCE, CYBERSECURITY AND ACCESS TO INSURANCE

Insurance People - The Superintendence of Private Insurance (Susep) published today in the Official Gazette of the Union Ordinances No. 8,323, No. 8,324 and No. 8,326, which establish Working Groups with the purpose of discussing and preparing technical studies related, respectively, to three fronts provided for in the 2023/2024 Regulatory Plan: Cybersecurity, Reinsurance and National Policy for Access to Insurance. Ordinance No. 8,323/2024 establishes a Working Group (GT) with the purpose of discussing and preparing technical studies on cybersecurity in the sector supervised by Susep and the challenges and opportunities that the development of the digital economy brings to the Brazilian insurance sector. The coordination will be carried out by Director Airton Almeida, from the Directorate of Prudential Regulation and Economic Studies.

BIG TECHS: TAX REFORM CREATES MARKET RESERVE IN CYBERSECURITY – BRAZIL

Digital Convergence - At a hearing at the Senate Economic Affairs Committee on Wednesday, August 28, entities representing information technology companies complained that a change made by the Chamber of Deputies in the tax reform creates a new market reserve in the country, now for cybersecurity services. "Companies with 20% national capital will have their tax rate reduced by 60%. In other words, it is creating a competitive asymmetry between companies here in Brazil. National companies will have a tax rate of 10.6%; companies that are not national will have a tax rate of 26.5%. But who are the cybersecurity companies that come to mind? They are multinationals. We are creating a market reserve", stated the director of government relations at Brasscom, Sérgio Sgobbi.

IDOPPRIL AND CNCS SIGN AGREEMENT IN FAVOR OF NATIONAL CYBERSECURITY – DOMINICAN REPUBLIC

The Caribbean - The Dominican Institute for the Prevention and Protection of Occupational Risks (IDOPPRIL) and the National Cybersecurity Center (CNCS) signed a cooperation agreement to carry out actions that promote and encourage a national cybersecurity culture, based on the effective protection of the Dominican State and its inhabitants. The agreement was signed by the executive director of IDOPPRIL, Dr. Fausto López Solís, and the head of CNCS, General of the National Police Juan Gabriel Gautreaux Martínez.

PERSONAL DATA LAW: SPECIALIST TALKS ABOUT PRIVATE PRESSURE TO MODIFY THE PROJECT – PARAGUAY

ABC - The bill on personal data protection was postponed due to pressure from companies, said cybersecurity specialist Miguel Ángel Gaspar, who also said that Paraguay should have had legislation protecting Internet and application users years ago. He recalled that in 2016 they had already presented at an event of the Internet Society, Paraguay chapter, the first investigation into Paraguayan applications that collected information from their users and that the need for legislation should be above particular interests.

MINISTRY OF SCIENCE AND INA LAUNCH CYBERSECURITY SCHOLARSHIP PROGRAM FOR WOMEN IN SMES IN COSTA RICA

The Feminist Diary - Recently, the Ministry of Science, Innovation, Technology and Telecommunications and the National Learning Institute (INA) of Costa Rica announced the launch of a scholarship program for women from small and medium-sized businesses and small and medium-sized agricultural producers. This initiative, called Cybersecurity Analyst for your Business: Women, seeks to strengthen the digital security of these types of productive units. The program offers 25 scholarships, which will cover 95% of the cost of the training provided with INA resources. The training consists of group and individual sessions totaling 57 hours over 11 weeks.

THE GLOBAL KALEIDOSCOPE OF MILITARY AI GOVERNANCE

UNIDIR - In the run-up to the second iteration of the Responsible AI in the Military Domain (REAIM) Summit, to be held in Seoul, Republic of Korea, on 9-10 September 2024, the Governments of the Republic of Korea and the Netherlands organized, in partnership with Chile, Costa Rica, Kenya, Singapore and Türkiye, a series of five regional consultations on responsible artificial intelligence in the military domain. This report captures UNIDIR's main reflections on the key takeaways stemming from the five regional consultations. These consultations did indeed enable the dissection of local contexts, realities and approaches with regard to the responsible development, deployment and use of AI in the military and wider security domains – including the identification of areas of nuanced convergence and divergence at the regional level.

THE NEW AI IMPERATIVE IS ABOUT BALANCING INNOVATION AND SECURITY

WEF - As AI dominates board discussions on global investment decisions, business leaders are often unaware of the cyber and digital risks their organizations face when adopting AI systems, as well as the strategies they should adopt to mitigate these risks. To stay competitive, organizations must encourage innovation, including the use of AI as a business enabler. However, focusing solely on AI's opportunities without addressing the associated cyber risks leaves organizations vulnerable. It is essential to consider the full cost of AI solutions, including security-related expenses. Rather than stifling innovation, cyber leaders should emphasize the importance of integrating security by design, implementing appropriate suites of cybersecurity controls and accounting for these costs to preserve business value.

GOVERNANCE OF ARTIFICIAL INTELLIGENCE IN THE MILITARY DOMAIN: A MULTI-STAKEHOLDER PERSPECTIVE ON PRIORITY AREAS (POLICY BRIEF)

UNIDIR - In March 2024, the Roundtable for AI, Security and Ethics (RAISE) was launched in Bellagio, Italy. A multi-year collaborative initiative led by UNIDIR and in partnership with Microsoft, RAISE is intended to establish itself as the neutral, trusted and independent platform for inclusive, cross-regional and multisectoral engagement on artificial intelligence (AI) in security and defence. The inaugural edition of RAISE convened participants primarily hailing from the industry and the research community, with select government representatives in light of the upcoming second edition of the Responsible AI in the Military Domain (REAIM) Summit (Seoul, 9-10 September 2024)

AI GOVERNANCE TRENDS: HOW REGULATION, COLLABORATION AND SKILLS DEMAND ARE SHAPING THE INDUSTRY

WEF - Artificial intelligence (AI) is transforming industries across the board as leaders recognize the technology's potential to improve productivity, enhance creativity, boost quality, and generate new solutions. This has created a surge in demand for AI, and in particular, generative AI. Unlocking the value of generative AI with responsible transformation can be a game-changer. Generative AI use cases can be found in various industries, from inspiring new designs in the furniture industry and personalizing marketing to accelerating drug discovery in the pharmaceutical industry.