DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 8, 2024

DIGI AMERICAS ALLIANCE MEMBERS

CYBER DEFENSE LABORATORY FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE IN CHILE INAUGURATED

EMOL - Thanks to a collaboration between the UC Innovation Center and the Chilean Army, the Cyberdefense Laboratory for the Protection of Critical Infrastructure was inaugurated, with the participation of prominent business associations and corporations. Entities such as the Association of Banks and Financial Institutions (ABIF), the Mining Cybersecurity Corporation (CCMIN), the National Electrical Coordinator (CEN), Conecta Logística of the Ministry of Transportation, CSIRT of the Government, the Catholic University through Dictuc - CETIUC, the UC Law, Science and Technology Program, Duoc UC, and technological allies such as Siemens, Scitum Claro, Lab X2X Claro, Amazon Web Services, Palo Alto Networks, DreamLab and Thales participate in this space, aimed at strengthening the defense of critical infrastructure.

CYBERCRIMES ARE ON THE RISE IN BRAZIL AND CYBERSECURITY IS A CHALLENGE FOR THE COMING YEARS

Tono Mural - The increasingly intense presence of the internet and social networks in our daily lives is undeniable. Data from the Brazilian Institute of Geography and Statistics (IBGE) reveals that 82% of Brazilian households have access to the internet. Brazil is also the third country in the world with the highest use of social networks. Fábio Matos, a sociologist specializing in forensic expertise, highlights the duality of digital communication. Although the internet offers access to information and opportunities, it can also be harmful when used inappropriately. "Digital communication is beneficial when it provides access to information and training. However, it is harmful when it leads to the loss of contact with people in everyday life," he states.

CHILE AND BRAZIL SIGN COOPERATION AGREEMENT ON CYBERSECURITY

TrendTIC - In a ceremony led by the Undersecretary of the Interior, Manuel Monsalve, and Marcos Antonio Amaro Dos Santos, Minister of State Head of the Institutional Security Cabinet of the Presidency of Brazil, both countries signed a memorandum of understanding (MOU) at La Moneda Palace, an agreement on cooperation in cybersecurity between both countries. This was within the framework of the Official Visit of President Luiz Inácio Lula da Silva to Chile that began on August 5. The agreement highlights the need to improve cybersecurity preparedness and manage risks, recognizing the importance of international cooperation. In addition, it seeks to promote cooperation and the exchange of information, based on shared values and human rights.

DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 8, 2024

COSTA RICA: MICITT AND INA LAUNCH CYBERSECURITY SCHOLARSHIP PROGRAM FOR WOMEN

Revista Summa - The Ministry of Science, Innovation, Technology and Telecommunications (MICITT) and the National Learning Institute (INA) announce the launch of the "Cybersecurity Analyst for your Business: Women" program, an initiative that offers 25 scholarships aimed at women from small and medium-sized enterprises (SMEs) and small and medium-sized agricultural producers (PYMPAS). The program aims to strengthen the digital security of these productive units and foster business resilience in today's cyber environment. This program, created by women for women, not only addresses cybersecurity needs but also promotes diversity and inclusion in the technology sector. The scholarships will cover 95% of the total cost of the program thanks to resources from INA, through its General SBD Scholarship Program. Each selected company must contribute the remaining 5%, equivalent to ₡56,100.00.

MEXICO LEADS IN GROWTH IN DEMAND FOR CYBERSECURITY SPECIALISTS

El Economista - In a context in which the demand for cybersecurity talent has cooled globally in the last year, Mexico has shown a reverse trend with an increase in the search for these specialized profiles, according to an analysis by LinkedIn Economic Graph. The demand for talent had an annual growth of 6.8% during 2024 in Mexico, a figure that exceeded the levels observed in economies such as Spain, India, the Netherlands, Australia and Germany, according to data from the professional network. In the case of our country, the behavior of the cybersecurity job offer is in line with the risks perceived by senior management. PwC's Digital Trust Insights 2024 shows executive concern about cyber threats.

THE NATIONAL PARTY FILED A COMPLAINT AGAINST AN ATTACK ON ITS WEBSITE: "WE WILL NOT LET ANYTHING GO" - URUGUAY

El Observador - The president of the National Party, Macarena Rubio, appeared this Tuesday at the Cybercrime Unit of the Ministry of the Interior to report the vulnerability incident suffered on the website of the political force in which a group of cybercriminals threatened Senator Graciela Bianchi. Through a statement they mention that the attack compromised the security of the website and although they assured that measures were implemented, the "seriousness of the incident" made evident the need for an intervention by the Cybercrime Unit.

CYBERSECURITY GUIDE FOR THE ENERGY SECTOR: HOW TO PROTECT DATA AND AVOID ATTACKS - DOMINICAN REPUBLIC

Energia Estrategica - In the Dominican Republic, as in many other parts of the world, electricity generation companies face significant risks related to cybersecurity in both their Information Technology (IT) and Operational Technology (OT). “These risks not only threaten the operational stability of companies, but also national security due to the critical importance of the electrical infrastructure,” warned Elsa Encarnación, Director of Cybersecurity and Cyberdefense of the Ministry of Defense of the Dominican Republic.

DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 8, 2024

HOW THE NATIONAL DIGITAL SECURITY CENTER RESPONDS TO CYBERATTACKS IN PERU

Andina - A ransomware attack that affected Ingemmet's digital services in July reversed advances in administrative simplification, returning to the in-person registration of mining applications only, and which - after two weeks - has not yet been reestablished virtually. Fortunately, 100% of the country's geological and mining information was protected. This has been one of more than 380 digital security incidents that have been detected and warned about this year by the National Digital Security Center of the Presidency of the Council of Ministers (PCM). Learn how this team of experts works to support public and private entities in cybersecurity.

AI COMPLACENCY IS COMPROMISING WESTERN SECURITY

ASPI - Just as the West has been forced into confrontation with Russia and China, military conflicts have revealed major systemic weaknesses in the US and European militaries and their defence-industrial bases. These problems stem from fundamental technology trends. In Ukraine, expensive manned systems such as tanks, combat aircraft and warships have proven extremely vulnerable to inexpensive unmanned drones, cruise missiles, and guided missiles. Russia has already lost more than 8,000 armored vehicles, a third of its Black Sea fleet and many combat aircraft, leading it to move its expensive manned systems farther from combat zones.

HOW TO MAKE MILITARY AI GOVERNANCE MORE ROBUST

War on the rocks - AI-enabled warfare has reached its “Oppenheimer moment.” From the backroom to the battlefield, AI is now being integrated into the full spectrum of military operations, including in logistics, intelligence collection, wargaming, decision-making, target identification, and weapons systems, with increasing levels of autonomy. The Ukrainian military is flying AI-enabled drones; the Israel Defense Forces are relying on AI to accelerate and expand targeting in Gaza; and the Pentagon is using AI to identify targets for airstrikes. The military AI revolution has arrived, and the debate over how it will be governed is heating up.

REFLECTING ON CYBER POWER: A LABOUR FUTURE?

RUSI - In 2021, the Integrated Review of Security, Defence, Development and Foreign Policy presented the UK’s ‘responsible, democratic’ view on cyber power that set out a strategic narrative and organising concept for future cyber policy. Amid the reassessment of priorities by the new government under its Strategic Defence Review, the concept and practice of cyber power must also be evaluated for its effectiveness. The Labour administration inherits a well-developed suite of strategic levers of cyber power, including institutions in the National Cyber Security Centre (NCSC) and the National Cyber Force (NCF) in addition to deep expertise across government. This commentary takes stock of the UK position on cyber power as a strategic narrative and organising concept, the challenges of promoting responsible and democratic use, and what this might mean for the new government.