DIGI AMERICAS LATAM CISO

INSIGHTS

NOVEMBER 15, 2024

MEXICO LAUNCHES NATIONAL CYBERSECURITY AND CLOUD PLAN TO BOOST DIGITAL TRANSFORMATION

Noti Press - The Government of Mexico, through the Digital Transformation and Telecommunications Agency, presented a project known as the National Cybersecurity and Cloud Plan Mexico. The central objective of this plan is to guarantee the security and resilience of government information systems, optimizing the use of technological infrastructure for more efficient and transparent administration. During the presentation of the project in the morning of November 14, 2024, Professor José Antonio Peña Merino, who leads the agency, explained that the initiative seeks to unify the technological capabilities of the government to achieve greater autonomy in the development of digital solutions. This not only allows for reducing operating costs, but also closing gaps in access to public services throughout the population.

INSECURITY AND CYBERCRIME SLOW THE DEPLOYMENT OF COMMUNICATION NETWORKS - MEXICO

El Financiero - In Mexico, telecommunications infrastructure is increasingly threatened by organized crime, which compromises the deployment of new generation networks such as 5G. Alfredo Pacheco, general director of the National Chamber of the Electronic Industry of Telecommunications and Information Technologies (Canieti), said that telecommunications companies face extortion and control of places that prevent the maintenance and expansion of networks, in addition to the installation of pirate networks using stolen infrastructure.

NOEMÍ LUNA CALLS FOR LEGISLATION ON CYBERSECURITY AFTER DETECTION OF THOUSANDS OF FAKE WEBSITES - MEXICO

Political Size - Deputy Noemí Berenice Luna, coordinator of the PAN Parliamentary Group, called on Morena to support the demands of experts and organizations to legislate on cybersecurity, since the lack of regulation in this area generates million-dollar losses due to fraud. She said that data from the Secretariat of Security and Citizen Protection (SSPC), through the National Registry of Cyber Incidents (RNIC), reveal that 3,888 fake websites were detected that posed as government agencies to obtain personal and financial data, with the aim of committing fraud or spreading malicious code.

COMMISSION APPROVES CYBERSECURITY AND PERSONAL DATA PROTECTION LAWS

El Salvador - After a series of modifications, the National Security and Justice Commission of the Legislative Assembly approved the Law on Cybersecurity and Information Security, as well as the Law on Personal Data Protection with only the contributions of the Secretariat of Innovation of the Presidency. The "Law on Cybersecurity and Information Security", which would seek to structure, regulate and supervise cybersecurity and information security measures held by public institutions, also creates the State Security Agency, also called "ACE".

ARMED FORCES TO ACT IN G20 SECURITY - BRAZIL

Agencia Brasil - The Eastern Military Command reported that the operation for the G20 Leaders' Summit - on November 18 and 19 - will involve resources from the Brazilian Navy, Army and Air Force, in cooperation with the state government, the city government, various agencies and public security agencies. The Army will employ approximately 7,500 men and women, who will work in activities such as: escorting authorities; perimeter security; protecting critical infrastructure; patrolling roads and areas; counterterrorism actions; electronic warfare; cyber defense; anti-aircraft defense; protection against drones; and chemical, biological, radiological and nuclear defense. Specialized resources and helicopters will be used.

THE COUNTRY CONSOLIDATES STRATEGIES TO STRENGTHEN COMPUTER SECURITY IN THE FINANCIAL SECTOR - COLOMBIA

MINTIC - In order to learn about new initiatives that strengthen cybersecurity in the financial sector, the ICT Minister, Mauricio Lizcano, today toured the facilities of the Operations Center of the Collaboration and Information Exchange Program of the Colombian financial sector and the Center of Excellence for Cybersecurity (CSIRT) of the Banking and Financial Entities Association of Colombia (Asobancaria). At the meeting, he ratified the importance of creating strategic alliances to strengthen the Colombian Cyber Emergency Response Group (Colcert) with the sectoral CSIRTs, and thus expand cybersecurity in the different sectors of the economy.

WHITE HOUSE CONFIRMS IT FINANCED PURCHASE OF PEGASUS SOFTWARE FOR COLOMBIA AMID FIGHT AGAINST DRUG TRAFFICKING

Week - This Thursday, the newspaper El Tiempo reported, based on sources from the White House in Washington and Bogotá, that the United States financed the acquisition of the Pegasus software for Colombia, in the midst of the fight against drug trafficking. "Two senior officials from Joe Biden's administration in Washington and another in Bogotá, officially authorized to speak on the subject, revealed exclusively to El Tiempo that the United States Government was not only aware of the purchase of the Pegasus software in Colombia but that, in addition, it was that country that financed its acquisition," reported the aforementioned newspaper. "To help ensure this proper use, strict protocols with checks and balances were established. The strict supervision of this tool was designed and implemented to ensure that the software was used to pursue legitimate objectives related to drug trafficking. We have no information to suggest that the software was misused to monitor Colombian political figures," said one of the sources, according to the news published by El Tiempo.

UNITED ARAB EMIRATES AND URUGUAY SIGN AGREEMENT TO PREVENT CYBER ATTACKS

Gub.Uy - On October 17, representatives of Agesic and the Cyber Security Council of the United Arab Emirates (UAE) signed a Memorandum of Understanding with the aim of strengthening cooperation between both countries for the detection and prevention of information security incidents. The agreement establishes a framework for collaboration between the UAE and Uruguay to facilitate the exchange of knowledge and good practices, as well as the development of joint capabilities in the field of cybersecurity.

FIRST EDITION OF THE URUGUAY CYBERSECURE TRAINING

Gub.Uy - The first edition of the Uruguay Ciberseguro training was held from November 6 to 8, with the aim of promoting teamwork among various public and private institutions, and developing cybersecurity skills through simulation exercises for responding to cyber incidents. The first edition of Uruguay Ciberseguro focused on practical exercises that promoted interaction between different teams, which allowed for comprehensive work on identifying, resolving and managing cyber incidents.

MORE THAN 60 STATE SITES INACCESSIBLE: WHAT HAPPENED AND WHEN WAS IT FIXED? - URUGUAY

Agesic assures that no information was lost in the incident and that it was a problem with access. Massive outage: More than 60 state websites, including ministries, DGI and the Electoral Court, were no longer accessible to citizens since Thursday at 3:00 p.m. In the morning they were restored. Agesic clarifies: The Electronic Government and Information Society Agency (Agesic) assured that the information was always safe; the problem was that access was down. Possible cause: Failure in two security devices.

FELABAN CLOSES WITH $40 BILLION IN BUSINESS AND CYBERSECURITY

Today - Edgar Alarcón, executive director of the Association of Banks of Paraguay (Asoban), made a positive assessment of this year's edition. "The assembly is ending with very positive results. The attendees are leaving very happy, with new experiences and learnings, especially regarding business and the future vision of the banking sector," said Alarcón in an interview with GEN. One of the recurring themes in the discussion panels was the impact of technology on the banking sector. Banking entities in the region, especially in Paraguay, are increasingly adopting technologies to offer better service to their clients.

LATIN AMERICAN COUNTRIES WILL STRENGTHEN CYBERSECURITY CAPABILITIES WITH SUPPORT FROM CHILE AND THE EUROPEAN UNION

EEAS - An agreement was signed at the La Moneda Palace to develop the triangular cooperation project “Strengthening and developing capacities in Latin America and the Caribbean in the area of cybersecurity”, which aims to increase the cyber resilience of Latin American countries, thus contributing to a safer and more stable digital environment at a global level. This initiative is part of the EU-LAC Digital Alliance that seeks to promote collaboration between the European Union and Latin America on key digital issues through dialogue and joint initiatives, fostering a human-centred digital transformation in both regions.

TSA PROPOSES NEW CYBERSECURITY RULES

ExecutiveGov - The agency said Wednesday the proposal will mandate cyber risk management and reporting requirements for particular surface transportation operators. Under the proposal, certain pipeline, freight railroad, passenger railroad and rail transit owners and operators are required to establish and maintain a cyber risk management program. The owners and operators of the surface transportation systems also need to report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency previously, they were only required to report to the TSA. Finally, each high-risk pipeline owner and operator will designate a physical security coordinator to report physical security issues to the TSA.

UNPACKING CYBER RESILIENCE - WEF REPORT

WEF - Resilience in the face of cyber risk is a critical objective for any organization dependent on digital technologies and data. This places it on the radar for almost all business leaders in 2024. The globalization of our supply chains, the complexity of technology stacks and the continued appetite to innovate with digital have led to continued aggregation of systemic cyber risk. Effective cyber resilience is complex. How we achieve it and the controls we use are highly context dependent; what works in the face of one type of threat may not work as well for another. For example, defending against ransomware is very different from defending against denial of service, and defending against accidental failures in a system requires different solutions from defending against a malign threat actor seeking to attack for reasons of sabotage, theft or financial gain.

HOW PIONEERING PUBLIC-PRIVATE COLLABORATION IN THE FINANCIAL SECTOR CAN HELP SECURE ITS QUANTUM FUTURE

WEF - Recent advancements in quantum computing have raised the technology’s role as a disrupter, significantly increasing the potential for actors in the financial sector to gain a competitive edge. Quantum technology promises breakthrough capabilities in algorithmic methodology such as portfolio optimization, Monte Carlo simulations and complex calculations, fueling projected investment growth from $80 million in 2022 to $19 billion by 2032. An increasing number of collaborations and research and development highlight financial services as a first mover in quantum computing. For example, JPMorgan Chase and PayPal are using IBM Quantum, to research optimization problems related to fraud detection.

COLLABORATIONS BETWEEN INDUSTRY EXPERTS AND THE PUBLIC SECTOR ARE DISRUPTING CYBERCRIMINALS. HERE’S HOW

WEF - An estimated 25.5% of the world’s population was impacted by cyber-enabled fraud in 2023. The impact of the profits this generates for criminals goes further than the immediate victims. In 2023, the United Nations reported that at least 220,000 people had been trafficked in South-East Asia, some from as far away as Africa and Latin America, and forced to run online scams. A new white paper from the World Economic Forum, Disrupting Cybercrime Networks: A Collaboration Framework explores how to build on the success of existing partnerships to accelerate the disruption of cybercriminal activities. Here we examine some of its learnings and recommendations.

THE UN CYBERCRIME CONVENTION THREATENS SECURITY RESEARCH. THE US SHOULD DO SOMETHING ABOUT IT

CyberScoop - The United Nations' recent adoption of a new cybercrime convention has sparked significant discussion within the global cybersecurity community. While the UN Convention Against Cybercrime aims to enhance international cooperation to combat malicious hacking, the convention raises serious concerns for those involved in security research and ethical hacking. The treaty's provisions related to security research conflict with best practices encouraged by the U.S. government and federal policies that protect good-faith security research from prosecution. Despite these and other concerns, the treaty is expected to receive final approval from the General Assembly by the end of the year.

WHAT COULD THE TRUMP ADMINISTRATION MEAN FOR CYBERSECURITY?

Information Week - The results of the 2024 US presidential election kicked off a flurry of speculation about what changes a second Donald Trump administration will bring in terms of policy, including cybersecurity. InformationWeek spoke to three experts in the cybersecurity space about potential shifts and how security leaders can prepare while the industry awaits change. In 2020, Trump fired Cybersecurity and Infrastructure Security Agency (CISA) Director Christopher Krebs after he attested to the security of the election, despite Trump's unsupported claims to the contrary. It seems that the federal agency could face a significant shakeup under a second Trump administration.