**DIGI AMERICAS ALLIANCE MEMBERS**

aws | Apple | CISCO | CLOUDFLARE | CROWDSTRIKE | fluid attacks we hack your software | Google | GRUPO RADICAL AVANT GARDE CYBERSTRATEGIES | LUMU | SISAP Sistemas Aplicativos

mastercard | netskope | paloalto NETWORKS | Telefónica | tenable | METABASE Q | Trellix | TREND MICRO | Santander

## ICT MINISTRY LAUNCHED THE CIBERPEACE PROGRAM THAT IS COMMITTED TO A SAFE, RESPECTFUL AND INCLUSIVE INTERNET – COLOMBIA

MINTIC - From the capital of the Atlantic, at the Autonomous University of the Caribbean and under the slogan "The Caribbean connects with CiberPeace", the National Government presented the CiberPeace program, which will reach the entire country, in search of promoting conscious use , empathetic, inclusive and responsible for Information and Communications Technologies, ensuring the participation of Colombians in the digital era. "CiberPeace will allow us to reach that deep Colombia, to those who do not have a voice, to those who do not appear in the major media or the major television networks. It will also allow us to build territory from the communities themselves" , highlighted Belfor García, Vice Minister of Digital Transformation of the ICT Ministry.

## CNMP ESTABLISHES THE NATIONAL CYBERSECURITY POLICY AND SYSTEM OF THE PUBLIC MINISTRY – BRAZIL

CNMP - The National Council of the Public Ministry published, this Wednesday, July 3, CNMP Resolution No. 294/2024, which establishes the Public Ministry's National Cybersecurity Policy and System (PNCiber-MP). The text, unanimously approved on May 28, during the 8th Ordinary Session of 2024, was presented by the national inspector of the Public Ministry, Ângelo Fabiano Farias, and reported by the then counselor Jayme de Oliveira. The resolution is made up of nine chapters, which deal with the general provisions, principles, objectives, instruments, governance and management of PNCiber-MP, the National Cybersecurity System, cybersecurity in units and branches and the strategy, MP's national cybersecurity plan and final provisions.

## CYBERSECURITY, PRIORITY OF MEXICAN BANKING; INVESTMENTS ARE COMING

Excelsior - Banks will invest around 24 billion pesos in cybersecurity and increasing digital offerings this year, according to the Association of Mexican Banks (ABM). Julio Carranza, leader of the bankers, highlighted that last year this same amount was allocated to protection against cybercriminals and the expansion of digital products derived from the accelerated adoption of online financial services. In his opinion, the level of investment should give certainty to banking users that financial institutions are committed to not suffering cyber attacks that compromise their operations. As well as offering a complete range of services via the internet.

# URUGUAY WILL STRENGTHEN DIGITAL GOVERNMENT SERVICES WITH SUPPORT FROM THE IDB

BNAmericas - The Inter-American Development Bank (IDB) approved a Conditional Credit Line for Investment Projects of US$74 million to increase the efficiency of public management, increase the level of security of the digital space and improve the management of the health system of Uruguay through strengthening digital government services. This Line of Credit to implement the "Digital Transformation Program for a Smart Country" includes a first individual loan of US$20 million. Although Uruguay has a very high level of digital government development, there is an opportunity to strengthen online government services, especially in the health sector, and to increase the capacity to detect and respond to incidents in cyberspace given the growing number of cyber threats to global level.

# MILITARY FORCES ARE IN THE PROCESS OF STRENGTHENING CYBERSECURITY – PARAGUAY

LaNacion - Following the announcement made by the traveling ambassador of the United States for Cyberspace and Digital Policy, Nathaniel Fick, about the cooperation of USD 3.1 million for the Armed Forces, the Minister of Defense Óscar González indicated that this is in full development and that thanks to this strengthening process, hacks could now be avoided. "The Technology detachment of the Military Forces was the one that alerted on one occasion a few months ago about an attempt or start of a hack into civil institutions, this department was the one that raised the alert at that time and thanks to that it could be quickly corrected. It was a very positive intervention by the respective leadership of the Military Forces and we are in the process of strengthening that area," said the Secretary of State.

# EXPERTS RAISE DEBATE ON SECURITY IN THE FACE OF GREATER DIGITAL BANKING – PARAGUAY

Breaking News - In recent years, Paraguay has experienced exponential growth in the adoption of digital banking. Although this trend has facilitated access to financial services and improved financial inclusion, it has also highlighted the need to guarantee the security of transactions carried out through these channels. In this sense, the increase in banking fraud such as account emptying, SIM swapping and phishing has generated concern among clients and authorities. In this regard, analyst and legal expert Stan Canova points out that digital banking is expanding by leaps and bounds, while other actors that must accompany this process in our country are advancing at a more tiring pace.

# MINISTRY OF DEFENSE WILL TRAIN PERSONNEL OF THE ARMED FORCES IN CYBERSECURITY – PERU

Gob:pe - The Ministry of Defense will train all personnel in the sector, active and retired military personnel, graduates and troops of the Armed Forces in the "Cyber Soldiers Program: Trained and empowered digital citizens on the cybersecurity route", which was launched today at the sector's institutional headquarters. The event was led by the Vice Minister of Defense Policies, César Torres Vega, representing Minister Walter Astudillo Chávez, in the presence of the Secretary General, María Chumbe Rodríguez; the head of the General Office of Technology, Information and Statistics (OGTIE), Ernesto Castillo, as well as representatives of allied companies.

## STUDY IN CYBERSECURITY: KEYS TO STRENGTHEN DIGITAL DEVELOPMENT IN CHILE

ReporteMinero - Strengthening the digital development of Chile, identifying areas of improvement to advance the information security of institutions and people, was the objective that drove the development of the study "Research and Development in Cybersecurity", mandated by the Ministry of Science , Technology, Knowledge and Innovation (MinScience). For the Undersecretary of the MinScience, Carolina Gainza, cybersecurity is a strategic priority "Cybersecurity is an issue of our present, which presents us with challenges and threats. "It is essential that we work together to strengthen our capabilities and develop innovative solutions that respond to these challenges."

## 70% OF NATIONAL ORGANIZATIONS DO NOT HAVE AN ADEQUATE BUDGET FOR CYBERSECURITY – COSTA RICA

CRHoy - 70% of Costa Rican organizations surveyed in an academic study affirm that the budget assigned to them is not adequate to current cybersecurity needs. This is clear from the State of Cybersecurity in Costa Rica 2023, prepared by the Cybersecurity Research, Development and Innovation Laboratory (LabCIBE) of the National University (UNA), whose results were obtained through a survey. In order to collect information about the allocated budget and the available resources that the company has to address cybersecurity issues in its organization's infrastructure, a specific section was assigned in the research, since investment in cybersecurity can be translated as preventive measures, detection systems and even response capacity, as well as training and training programs.

## CYBERSECURITY IN LATIN AMERICA WILL REACH USD$1,708 MILLION

Market - The managed cybersecurity services market in Latin America is experiencing significant growth. According to a report by Frost & Sullivan, the market is expected to reach USD 1,708 million by 2024, which represents a growth of 12.8% compared to 2023. It should be noted that managed cybersecurity is a set of solutions that offers a specialized external company to another to manage your digital security. In this context, one of the main drivers of this growth is the lack of qualified personnel.

## NEW TAX ALLOWANCE TO BOLSTER CYBER SECURITY – T&T

Newsday - In a significant move to enhance the cyber security framework of TT, the National Information and Communication Technology Company Ltd (iGovTT), under the Digital Transformation Ministry, launched the Cybersecurity Investment Tax Allowance (CITA) management system on June 12. This initiative, part of the broader Cybersecurity Tax Administrative System (CySTAMS), was originally announced by Finance Minister in the 2023/2024 national budget. According to iGovTT, the platform allows businesses to submit proof of their cyber security purchases for validation, enabling them to claim tax credits up to $500,000 from the Inland Revenue Division of the Ministry of Finance.

## MEKOTIO BANKING TROJAN THREATENS FINANCIAL SYSTEMS IN LATIN AMERICA

TrendMicro - The Mekotio banking trojan is a sophisticated piece of malware that has been active since at least 2015, primarily targeting Latin American countries with the goal of stealing sensitive information — particularly banking credentials — from its targets. Originating in the Latin American region, it has been particularly prolific in Brazil, Chile, Mexico, Spain, and Peru. Furthermore, Mekotio seems to share a common origin with other notable Latin American banking malware such as Grandoreiro, which was disrupted by law enforcement earlier this year. Mekotio is often delivered through phishing emails, employing social engineering to trick users into interacting with malicious links or attachments.

## OPERATION REGULATION: STRENGTHENING LATIN AMERICA'S AI GOVERNANCE

ECFR - Recent elections in Latin America have underscored the dangerous impact of algorithms and AI, particularly generative AI, at the voting booth. During the 2023 Colombian regional election, campaigns were marred with misinformation funnelled across social media, with the emergence of AI-generated media content – or deepfakes – aimed at undermining candidates' political campaigns. This raised alarm bells among fact-checking groups like ColombiaCheck, as the widespread and convincingly realistic recordings enabled by generative AI's mimicry proved too difficult and time consuming to debunk before some damage was already done. A similar hoax sprung up during Argentina's 2023 election, where candidate Patricia Bullrich was the target of AI-generated audios slandering her minister of economy. In the recent Mexican election, a deepfake audio of candidate Claudia Sheinbaum mimicked her criticising President Andrés Manuel López and acknowledging fraud in the polls.

## UNVEILING SUSPICIOUS PHISHING ATTACKS: ENHANCING DETECTION WITH AN OPTIMAL FEATURE VECTORIZATION ALGORITHM AND SUPERVISED MACHINE LEARNING

Frontiers - The dynamic and sophisticated nature of phishing attacks, coupled with the relatively weak anti-phishing tools, has made phishing detection a pressing challenge. In light of this, new gaps have emerged in phishing detection, including the challenges and pitfalls of existing phishing detection techniques. To bridge these gaps, this study aims to develop a more robust, effective, sophisticated, and reliable solution for phishing detection through the optimal feature vectorization algorithm (OFVA) and supervised machine learning (SML) classifiers.

## HOW NATIONS CAN BUILD SOVEREIGN AI AND HOMEGROWN TALENT FOR ECONOMIC COMPETITIVENESS

WEF - Artificial intelligence is intellectually driven, not policy driven. It's about the people, and these are the people that build the foundation of what makes an AI ecosystem. The tech and algorithms in AI have been commoditized, but AI ecosystems become fully functioning when every stakeholder is aligned towards building the next generation of AI talent to populate their local ecosystems. Examples can already be seen across the United States. In December 2023, the state of New Jersey, NJEDA and Princeton University launched the NJ AI Hub for AI innovation and, a month later, the state of New York launched Empire AI, a state-of-the-art computing centre for ethical artificial intelligence (AI) research in collaboration with New York University, Columbia University and five other institutions.

## HOW COMPANIES CAN MITIGATE AI'S GROWING ENVIRONMENTAL FOOTPRINT

HBR - By 2026, computing power dedicated to training AI is expected to increase tenfold. As more power is expended, more resources are needed. As a result, we've seen exponential increases in energy and perhaps more unexpectedly, water consumption. Some estimates even show running a large AI model generates more emissions over its lifetime than the average car. A recent report from Goldman Sachs found that by 2030, there will be a 160% increase in demand for power propelled by AI applications.

## NOW THE EU COUNCIL SHOULD FINALLY UNDERSTAND: NO ONE WANTS "CHAT CONTROL"

EFF - The EU Council has now passed a 4th term without passing its controversial message-scanning proposal. The just-concluded Belgian Presidency failed to broker a deal that would push forward this regulation, which has now been debated in the EU for more than two years. For all those who have reached out to sign the "Don't Scan Me" petition, thank you—your voice is being heard. News reports indicate the sponsors of this flawed proposal withdrew it because they couldn't get a majority of member states to support it.