DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 23, 2025

THE ICT MINISTRY INAUGURATED THE COLOMBIAN NATIONAL SECURITY OPERATIONS CENTER (SOC) TO PROTECT THE CYBERSECURITY OF THE COUNTRY'S ENTITIES

MinTIC - Thinking about preventing, managing and responding quickly to cybersecurity incidents and emerging threats, strengthening knowledge on the subject and promoting a culture of protection in the digital environment, the ICT Minister, Mauricio Lizcano, inaugurated the National Security Operations Center (SOC). This initiative, led by the Colombian Cyber Emergency Response Group (ColCERT) of the ICT Ministry and supported by key entities of the country's digital ecosystem, is a key pillar of the national cybersecurity strategy.

FEDERAL POLICE LAUNCH OPERATION AGAINST GANG SPECIALIZING IN FRAUD AT CAIXA - BRAZIL

SBT News - The Federal Police (PF) launched Operation Chaes on Wednesday (22) with the aim of dismantling a criminal group specialized in financial fraud. The scheme mainly affected Caixa Econômica Federal customers, but other banking institutions were also targeted by the gang. The investigation, which had the support of the Coordination for the Repression of High Technology Crimes (CCAT), revealed that the group used a sophisticated malware called Chaes.

WHAT DOES 5G BRING TO CYBERSECURITY? KEYS TO UNDERSTANDING THE CHALLENGES AND OPPORTUNITIES - COSTA RICA

La Republica - The arrival of 5G represents a paradigm shift in digital connectivity, offering greater speed, lower latency and an unprecedented capacity to connect devices. However, this technological advance also brings with it significant challenges in terms of cybersecurity, according to the Chinese Embassy in Costa Rica.

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 23, 2025

PN ADVANCES IN THE ORGANIZATIONAL DESIGN OF THE CYBERSECURITY AREA DIRECTORATE - DOMINICAN REPUBLIC

CDN - The National Police (PN) held the third coordination meeting for the creation of the Cybersecurity Area Directorate, in a meeting held in the Strategic Thinking Room of the Central Planning and Development Directorate (Diplan). The meeting's main objective was to fine-tune the strategic and organizational details of this new department, designed to protect the institution's equipment, systems, data and networks.

US SANCTIONS CHINESE FIRM THAT SUPPORTED CYBER ESPIONAGE IN PARAGUAY

Breaking News - A cyberespionage group based in the People's Republic of China, identified as Flax Typhoon, infiltrated the Paraguayan government's systems just over a month ago. The Treasury Department's Office of Foreign Assets Control (OFAC) updated its blacklist of individuals, entities, and vessels that the United States Government considers to threaten the country's national security or foreign policy.

MEXICO MUST WORK MORE ON CYBERSECURITY AND ARTIFICIAL INTELLIGENCE ISSUES TO STOP VIOLENCE

Metropolis - Mexico needs to send good signals abroad, that it is working to combat fentanyl, corruption, impunity, because Mexico remains in a serious crisis of violence from organized crime, mainly in what refers to high-impact criminal violence and that associated with criminal disputes for territorial control. In a press conference, security experts conducted an analysis of Security 2025, a Multidisciplinary analysis, where they warned that Mexico must work on cybersecurity issues, it urgently needs support in terms of security, "because it has not been able to solve its violence problem."

PACHUCA CITY HALL STRENGTHENS CYBERSECURITY AFTER HACKING ATTEMPT - MEXICO

am - Following an alleged hacking attempt on the systems of the Pachuca City Council, municipal authorities issued a statement to inform about the measures they will apply in order to avoid risks. The document indicates that there will be immediate protection, since since the detection of the incident, advanced cybersecurity protocols directed by specialists from the IT Department were activated, which has allowed the protection of the systems and reduced risks.

CYBERSECURITY AND ARTIFICIAL INTELLIGENCE TRENDS FOR 2025

Merca2.0 - The advance of artificial intelligence (AI) and cyber threats has brought companies to a tipping point where they must adopt innovative strategies to stay protected... Identified seven key predictions that will shape the future of cybersecurity in 2025, highlighting the convergence of AI and unified platforms as drivers of change.

FAKE REALITY AND IDENTITY: A NEW CYBERSECURITY CHALLENGE

Debate - Cybersecurity experts predict that 2025 will see a major leap in the use of artificial intelligence and 'deepfakes' (extremely realistic fake videos), data theft will experience a significant jump evolving into mass identity theft, and sophisticated scams and new financial fraud tactics will emerge.

COORDINATION AND GOVERNANCE IN CYBERSECURITY: NEW REGULATORY AND OPERATIONAL FRAMEWORK - EU

CincoDias - NIS-2 and DORA regulations reinforce the obligation to supervise critical suppliers, unifying the responsibility of these entities with the comprehensive management of their digital ecosystem. New year, new challenges and new regulations: NIS-2 and DORA. Changes are coming, and with them, doubts. It is time to generate certainty. It is time to generate growth. Let's address key ideas, both legal and operational, that will boost efficiency in corporate management.

CYBERSECURITY IN TRANSITION: BIDEN ADMINISTRATION WARNINGS AND WHAT’S NEXT FOR THE U.S.

Govtech - From a new White House executive order on cyber to a blog from the outgoing CISA director to more scary details on the Treasury hack, the outgoing administration has strong words on cyber threats. As President Joe Biden and his team of appointed senior executives across the federal government packed their bags and prepared to vacate offices inside the D.C. Beltway, one of their strongest messages proclaimed in their final days was this: "Pay attention on all things cybersecurity." President-elect Donald J. Trump takes the oath of office (for the second time) at noon EST on Monday, Jan. 20, 2025. Meanwhile, the Biden administration sent a string of last-minute directives and warnings regarding cybersecurity over this past week.

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 23, 2025

TRUMP REVOKES BIDEN EXECUTIVE ORDER ON ADDRESSING AI RISKS - US

Reuters - U.S. President Donald Trump on Monday revoked a 2023 executive order signed by Joe Biden that sought to reduce the risks that artificial intelligence poses to consumers, workers and national security.
Biden's order required developers of AI systems that pose risks to U.S. national security, the economy, public health or safety to share the results of safety tests with the U.S. government, in line with the Defense Production Act, before they were released to the public.

COMMONWEALTH FELLOWS DEVELOP ROADMAP TO COMBAT CYBERCRIME IN CARIBBEAN

The Commonwealth - Commonwealth Caribbean cyber fellows have developed a roadmap this week, designed to boost around-the-clock cooperation to combat online crimes and make the internet safer for citizens.
The roadmap was the result of two days of discussions among 15 fellows, including officials from The Bahamas, Barbados, Grenada, Guyana, Jamaica, Trinidad and Tobago, the CARICOM Implementation Agency for Crime and Security, and the Regional Security System. The roadmap lays out a framework for greater regional cooperation to prevent and combat cyber threats, including fraud, ransomware, and hacking.

“ARTIFICAL INTELLIGENCE AND CYBERSECURITY: BALANCING RISKS AND REWARDS” WHITE PAPER

WEF - Cyber risks related to AI adoption have to be considered by business leaders and senior risk owners alike. This report is part of a series exploring the transformative role of artificial intelligence (AI) across industrial ecosystems, along with cross-industry, industry-specific and regional perspectives. It is specifically focused on how organizations can reap the benefits of AI adoption while mitigating the associated cybersecurity risks. The business benefits of adopting AI can be considerable, but the cyber risks of embedding these technologies into an organization are not always considered from the outset. By adopting AI, businesses may find themselves vulnerable to new threats that they do not yet know how to defend themselves against.

RESTORING TRUST ONLINE: WHAT CAN WE LEARN FROM CYBERSECURITY'S ZERO TRUST MODELS?

WEF - In recent years, cybersecurity engineers have been shifting into a new security model called “zero trust”: the idea that trust should not be automatically granted to any user or device by default. This stance has not yet been adopted by digital societies. Online users often bypass the information verification step, as evident from the global rise of false and misleading information. By adopting principles from zero trust models, online users could use the power of emerging AI technology, together with human moderation, and blockchain technology to become better at verifying information.