DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 1, 2025

DIGI AMERICAS ALLIANCE MEMBERS

GUYANA TO STRENGTHEN CYBERSECURITY AGAINST CYBERCRIME

Prensa Latina - The Guyanese government today aims to consolidate its digital development, which must be accompanied by the latest in cybersecurity to combat cybercrime. In this regard, Prime Minister Mark Phillips urged all sectors to be aware of the threats in this field, hence the importance of acquiring skills and equipping themselves with the necessary tools to protect national systems.

PRESIDENT ARÉVALO INAUGURATES THE CYBER EXERCISE "DEFENSE OF THE SOUTH 2025" - GUATEMALA

Guatemalan News Agency - President Bernardo Arévalo participated this Saturday in the inauguration of the cyber exercise known as Defensa del Sur 2025. This exercise is part of the Centam Guardian 2025 program and is part of a broader series of joint events aimed at improving the interoperability, operational coordination, and resilience of allied forces against multi-domain threats.

THE GUATEMALAN FOREIGN MINISTRY WAS HACKED BY A CHINESE SPY GROUP

infobae - The Guatemalan Ministry of Foreign Affairs' computer system was hacked by "cyber-espionage groups based" in China, the U.S. Embassy in the country reported Tuesday. "A joint cybersecurity review between Guatemala and @Southcom identified that the entire computer system was hacked by cyber-espionage groups based in the People's Republic of China," the embassy said in a message on its official X account.

DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 1, 2025

ARMY GENERAL STAFF INTEGRATES CYBER DEFENSE INTO THE ASTROS SYSTEM - BRAZIL

Air & Naval Defense - In compliance with the National Defense Strategy, which in 2008 established three strategic sectors for national defense: nuclear, space and cyber, the Ministry of Defense (MD) assigned responsibility for the development of the cyber sector to the Brazilian Army, under the coordination of the 2nd Sub-Chief of the Army General Staff.

CYBERSECURITY IN BRAZIL: HOW COMPANIES CAN PROTECT THEMSELVES IN ONE OF THE MOST ATTACKED COUNTRIES IN THE WORLD

Segurança Eletrônica - Brazil occupies an alarming position in the global cybersecurity scenario: it is the second country that suffers the most cyberattacks in the world. The increasing digitalization of businesses, combined with vulnerabilities in data protection, makes companies in all sectors frequent targets of cybercriminals. But how can organizations protect themselves from increasingly sophisticated threats?

RED ELÉCTRICA ESPAÑOLA RULES OUT A CYBERSECURITY INCIDENT AT ITS FACILITIES.

CB24 - After analyzing the blackout that occurred on Monday, Red Eléctrica concludes that "there was indeed no intrusion into the control systems that could have caused the incident." The massive power outage that affected mainland Spain caused economic losses of €1.6 billion, equivalent to 0.1% of gross domestic product (GDP), according to calculations by the country's main business confederation, the CEOE.

MAGNIFYING GLASS ON SPAIN'S QUANTUM TECHNOLOGY STRATEGY: HOW MUCH, HOW, AND WHY

dplnews - Spain launched its Quantum Technologies Strategy with two core objectives: to strengthen its quantum ecosystem, both in research and the market, and to prepare society for the changes these technologies entail. It will allocate a budget of €808 million from the European Regional Development Fund (ERDF) and the Recovery Plan; the potential for investment from the private sector is estimated at €1.5 billion.

HOW TAIWAN IS STRENGTHENING ITS CYBERSECURITY IN THE FACE OF CHINA'S MANEUVERS

infobae - On April 15, President Lai Ching-te presented the new national strategy for 2025 at CYBERSEC, Asia's largest cybersecurity conference, in response to China's latest military maneuvers in the Taiwan Strait. In his speech, he revealed that government systems would suffer 2.4 million cyberattacks per day in 2024, double the number from the previous year. Recent "CrazyHunter" ransomware attacks affected hospitals, schools, and businesses, with Chinese hackers identified as the perpetrators.

DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 1, 2025

GENERATIVE ARTIFICIAL INTELLIGENCE: OPPORTUNITIES AND RISKS FOR CYBERSECURITY

Portal Innova - The rise of Generative Artificial Intelligence (GAI) is marking a turning point in the field of cybersecurity. Generative AI-based cybersecurity solutions allow for the automation of incident documentation, accelerated threat search and analysis, interpretation of large volumes of log data, and the generation of awareness and cultural change campaigns. To increase productivity, companies have begun incorporating tools such as ChatGPT, Copilot, Claude 3, and Gemini.

NEW BILL MANDATES CYBERSECURITY OVERHAUL FOR FEDERAL CONTRACTORS - USA

Fortra - New cybersecurity legislation is coming thick and fast. And for good reason: cyber threats are becoming more sophisticated, systems are becoming more connected, and geopolitical relationships are becoming more fraught. One of the most recent bipartisan legislations – the US Federal Contractor Cybersecurity Vulnerability Reduction Act of 2025 – is designed to modernize cybersecurity standards in the US and protect the country from threats.

CISOS BAND TOGETHER TO URGE WORLD GOVERNMENTS TO HARMONIZE CYBER RULES

Cybersecurity Dive - A letter from the CISOs of 45 powerful global companies could provide crucial backing for world governments looking to reduce cybersecurity regulations and their accompanying hassles for businesses. The CISO letter, sent to members of the Group of Seven nations and the Organization for Economic Cooperation and Development, urges governments to use those high-level forums to “focus on greater alignment of cybersecurity regulations.”

ISC2 UNVEILS COMPREHENSIVE GUIDE FOR CYBERSECURITY IN SATELLITE COMMUNICATIONS

Industrial Cyber - The ISC2 has released a guide for cybersecurity practitioners to support their evaluation of the risks, challenges and use cases for privatized satellite-based communications (SATCOM). Satellite communications (SATCOM) have become more accessible than ever, with consumer mobile devices now able to connect to these networks.

CSIS 2025 SPACE THREAT ASSESSMENT: CYBERATTACKS ON SPACE SYSTEMS PERSIST, TRACKING HARDER AMID INFRASTRUCTURE THREATS

Industrial Cyber - The Center for Strategic & International Studies (CSIS) has released the 2025 Space Threat Assessment, noting that the authors find it increasingly difficult to track the year-over-year number of cyberattacks targeting space systems. Though their numbers differ, some organizations try to keep tallies of cyberattacks by the type of entity and sector targeted, among other criteria.

AS LATIN AMERICA BECOMES THE WORLD'S FAST GROWING REGION FOR NEW CYBERSECURITY ATTACKS, MARKETS LOOK TO AI FOR SOLUTIONS

Latin America Reports - According to a report from the World Bank, Latin America and the Caribbean recently became the world's fastest-growing region for disclosed cyber incidents, with a 25% average annual growth rate in the last decade alone. Furthermore, according to the international financial institution it is also the least protected region.

WEF, UNIVERSITY OF OXFORD PUBLISH CYBER RESILIENCE COMPASS WITH SEVEN PATHWAYS TO BUILD ROBUST CYBERSECURITY ROADMAPS

Industrial Cyber - The World Economic Forum (WEF), in collaboration with the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, released the Cyber Resilience Compass: Journeys Towards Resilience report on Thursday. The practical guide is designed to help organizations develop stronger cyber resilience strategies and navigate today's increasingly complex threat landscape with confidence. Drawing on frontline practices from leading organizations worldwide, the white paper offers actionable insights to support the creation of more effective and resilient cybersecurity roadmaps.

159 CVES EXPLOITED IN Q1 2025 — 28.3% WITHIN 24 HOURS OF DISCLOSURE

The Hacker News - As many as 159 CVE identifiers have been flagged as exploited in the wild in the first quarter of 2025, up from 151 in Q4 2024. "We continue to see vulnerabilities being exploited at a fast pace with 28.3% of vulnerabilities being exploited within 1-day of their CVE disclosure," VulnCheck said in a report shared with The Hacker News. This translates to 45 security flaws that have been weaponized in real-world attacks within a day of disclosure. Fourteen other flaws have been exploited within a month, while another 45 flaws were abused within the span of a year.