DIGI AMERICAS LATAM CISO

INSIGHTS

SEPTEMBER 25, 2025

DIGI AMERICAS ALLIANCE MEMBERS

Apple aws Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks we hack your software

Google kriptos LUMU netskope paloalto NETWORKS Resecurity

Schneider Electric SISAP Sistemas Aplicativos Strike Telefónica tenable Trellix TREND MICRO

CYBERSECURITY IN THE DOMINICAN REPUBLIC: 2030 STRATEGY, FIGURES, AND KEY ACTIONS TO SECURE THE DIGITAL ENVIRONMENT

Revista Mercado - Cybersecurity in the Dominican Republic has become a national priority in the face of the accelerated growth of digital threats affecting both the public and private sectors. In the first half of 2025, the Dominican Republic was the target of more than 233 million cyberattack attempts, with a recognition rate reaching 36,000 attempts per second. Faced with this situation, the country has responded with concrete actions such as the signing of inter-institutional agreements and the implementation of the National Cybersecurity Strategy 2030, which includes more than 50 specific activities and seeks to consolidate a secure, inclusive, and trustworthy digital environment, positioning the Dominican Republic as a regional leader in digital defense.

THE NATIONAL CYBERSECURITY AGENCY APPROVES THE PRELIMINARY LIST OF CRITICAL OPERATORS AND BEGINS PUBLIC CONSULTATION - CHILE

Carey - On September 16, 2025, the National Cybersecurity Agency (ANCI) approved the preliminary list of Vitally Important Operators (VIOs) for the first qualification process under Law No. 21,663, the Cybersecurity Framework. This resolution constitutes a milestone in the implementation of the new regulatory framework, as it identifies the entities required to comply with enhanced requirements for the protection of essential services.

CHILE: PUBLIC HEALTH SECTOR AND SME SUPPLIERS LAG MOST BEHIND IN CYBERSECURITY

Diario de Valdivia - Beyond the regulations, the weakness lies in the proactive protection and prevention of attacks, in addition to the absence of a consistent investment strategy for cybersecurity in both sectors. Oversight and mandatory self-reporting are essential parts of the new regulations. The breach of the Ministry of Health's platforms in 2016 and the Institute of Public Health this year are examples of the need to strengthen cybersecurity in the public health sector, as well as in the small and medium-sized businesses that supply it.

"HIGH DEMAND AND ELECTRICITY DEPENDENCE": THE CHALLENGES FACING CHILE DUE TO ENERGY CONSUMPTION FROM NEW TECHNOLOGIES - CHILE

TrendTIC - Today, new technologies, the massive proliferation of mobile devices (IoT), and the breakthrough advances in AI are significantly increasing dependence on energy generation. More than a warning, this represents a series of crucial challenges. According to the International Energy Agency (IEA), global energy demand will grow by 2.2% in 2024, exceeding the average for the last decade. This increase accounted for 4.3% of electricity demand, driven by record temperatures, electrification, and digitalization. In this last aspect, the expansion of data centers plays a fundamental role.

CYBERSECURITY IN THE ELECTRICITY SECTOR: HOW TO PROTECT THE BRAZILIAN SYSTEM FROM VIRTUAL ATTACKS - BRAZIL

Cenario Energia- With the digitalization of networks and the advancement of smart grids, experts warn of the risks of cyberattacks that could cause blackouts, millions in losses, and threaten energy reliability in Brazil. The digital transformation of the electricity sector has brought efficiency gains, but it has also opened new opportunities for cyberattacks.

GEOPOLITICS OF THE FUTURE: OUTER SPACE AND CYBERSPACE AS NEW HEARTLANDS - BRAZIL

Defesa em Foco - In the 20th century, power was disputed on land, sea, and air. But in the 21st century, geopolitics is expanding into new territories: outer space and cyberspace. Whoever dominates these domains can influence not only countries but the entire international system. Outer space, once the stage for the space race between the United States and the Soviet Union, has become a permanent strategic domain. Today, communication, observation, and navigation satellites are fundamental to the functioning of the global economy, from financial transactions to precision agriculture.

MGI PARTICIPATES IN CYBERSECURITY EXERCISE IN PREPARATION FOR COP 30 - BRAZIL

Gov.br - The Ministry of Management and Innovation in Public Services (MGI) participated last week in the 7th edition of the Cyber Guardian Exercise, considered the largest in the Southern Hemisphere focused on cyber defense. This year, the event featured 160 institutions and took place simultaneously in Brasília (DF) and Belém (PA), which will host the 30th UN Climate Change Conference (COP30) in November 2025. The Cyber Guardian exercise simulates incidents that compromise the functioning of critical infrastructure or essential services, and protocols for responding to these incidents and mitigating their effects are developed and trained. This year's exercise also included the Thematic Office module - Submarine Cables and Gov.br Domain, in which the MGI acts as one of the coordinators, simulating possible attacks that threaten national security or sovereignty.

DIGI AMERICAS LATAM CISO

INSIGHTS

SEPTEMBER 25, 2025

THE U.S. SEEKS TO BRING CHIP MANUFACTURING "BACK HOME" WITH SUPPORT FROM MEXICO

DPL News - The United States government is seeking to "bring manufacturing back home." It is currently working on this and needs "Mexico to play a key role in that process," stated Mark Johnson, Deputy Chief of the Trade Mission at the U.S. Embassy in Mexico. The Chargé d'Affaires of the U.S. Embassy, Johnson, asserted that the United States "will not tolerate dependence on countries like China for critical technology," such as semiconductors. In that regard, he congratulated the Mexican government for the tariffs it recently imposed on countries with which it does not have a trade agreement.

LATIN AMERICAN GOVERNMENTS FACE TECHNOLOGICAL AND CYBERSECURITY CHALLENGES IN THEIR OWN DATA CENTERS: DIGI AMERICAS

DPL News - Government data centers present challenges, and Latin America is no exception. Digi Americas published the report "The Challenges of Government Data Centers in Building Resilient Digital Infrastructures," which addresses a paradox in Latin American digital infrastructure policy: the belief that building and operating government-owned data centers is the best way to protect sensitive information.

SECRET SERVICE SAYS IT DISMANTLED EXTENSIVE TELECOM THREAT IN NYC AREA - USA

Cyberscoop - he Secret Service said Tuesday that it disrupted a network of electronic devices in the New York City area that posed imminent telecommunications-based threats to U.S. government officials and potentially the United Nations General Assembly meeting currently underway. The range of threats included enabling encrypted communications between threat groups and criminals, or disabling cell towers and conducting denial-of-service attacks to shut down cell communications in the region.

CISA SHARES LESSONS LEARNED FROM AN INCIDENT RESPONSE ENGAGEMENT - USA

CISA - CISA began incident response efforts at a U.S. federal civilian executive branch (FCEB) agency following the detection of potential malicious activity identified through security alerts generated by the agency’s endpoint detection and response (EDR) tool. CISA identified three lessons learned from the engagement that illuminate how to effectively mitigate risk, prepare for, and respond to incidents: vulnerabilities were not promptly remediated, the agency did not test or exercise their incident response plan (IRP), and EDR alerts were not continuously reviewed.

HEALTHCARE CYBERSECURITY: THE URGENCY OF NOW

Forbes - Healthcare exists at the intersection of trust and vulnerability. Every medical record, test result, and insurance claim is more than just data on a computer; it represents a person's identity, medical history, and, in many cases, the road to care. For years, I've warned in papers and briefings that the healthcare sector is particularly vulnerable. The most recent figures confirm that warning: healthcare breaches remain among the most common and costly in any business, and the gap between where healthcare security is and where it needs to be is expanding.