DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 10, 2026

DIGI AMERICAS ALLIANCE MEMBERS

PERU WILL HOLD ITS FOURTH NATIONAL CYBERATTACK SIMULATION TO STRENGTHEN THE COUNTRY'S DIGITAL SECURITY

gob.pe - In order to strengthen preparedness and response capabilities to digital security incidents, the Presidency of the Council of Ministers (PCM), through the Secretariat of Government and Digital Transformation, will hold the Cyberattack Simulation 2026 – SIMAC 2026 – next Thursday, July 16. This national exercise will bring together public and private entities to evaluate their detection, analysis, containment, recovery, and coordination procedures in the face of realistic cyberattack scenarios.

DIGITAL PAYMENTS AND CYBERSECURITY: THE CHALLENGE THAT CHILE CANNOT POSTPONE

Forbes Chile - In Chile, the growth of digital payments has been steady and significant. Over the last decade, their use has quadrupled, reaching more than 370 transactions per person per year, according to figures from the Central Bank of Chile. Furthermore, the transaction volume now exceeds 100% of GDP, according to the same institution's Payment Systems Report, reflecting a level of adoption that places the country among the most advanced in the region.

CYBERSECURITY EXPERT ON THE NEW PERSONAL DATA PROTECTION LAW: "THE DIOGENES SYNDROME OF COMPANIES WITH OUR DATA IS OVER" - CHILE

Futuro.cl - December 1, 2026, will mark a turning point in the privacy of Chileans with the entry into force of the new Personal Data Protection Law. This legislation not only creates a specialized agency but also transforms the nature of our information: data will now be considered the property of citizens, requiring explicit consent for any processing.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 10, 2026

SENATE CREATES PARLIAMENTARY FRONT FOR ARTIFICIAL INTELLIGENCE - BRAZIL

Poder360 - The Federal Senate has created the Mixed Parliamentary Front for Artificial Intelligence, Data Protection and Digital Security. Resolution No. 19 of 2026 was enacted by the President of the Senate, Davi Alcolumbre (União Brasil-AP), and published in the DOU (Official Gazette of the Union) this Friday (July 10, 2026). Read the full text (PDF – 287 KB). The new body is supra-partisan, non-governmental in nature, and of indefinite duration. The front brings together senators and federal deputies who sign the minutes of installation, with the possibility of later adhesion by other congressmen.

CYBER GUARDIAN 2026 WILL BRING TOGETHER MORE THAN 240 ORGANIZATIONS IN A NATIONAL SIMULATION OF DIGITAL ATTACKS - BRAZIL

Accounting - The Cyber Guardian Exercise 2026 (EGC 2026) will be held between September 21 and 25, bringing together more than 240 organizations in a national simulation of defense against cyberattacks. Considered the largest cyber defense exercise in the Southern Hemisphere, the event will include the participation of the Armed Forces, government agencies, regulatory agencies, educational institutions, and companies responsible for the country's critical infrastructure.

BRAZIL, DATA CENTERS, AND GROWTH OPPORTUNITIES

Be News - The global race for data processing capacity, accelerated by the exponential growth of artificial intelligence, is driving large investments in infrastructure. These measures are necessary for the operation of industrial-scale data centers, which consume from 100 to hundreds of megawatts and demand reliable power, high-speed connectivity, and physical and cybersecurity. These units are being urgently installed in countries that have the right conditions. A study by the Getúlio Vargas Foundation (FGV) presented this week demonstrates that a single 100 MW project can add R$ 1.5 billion to Brazil's GDP and generate 12,560 direct and indirect jobs. Brazil has real structural advantages to attract these investments. What is still lacking—and what the study honestly identifies—is the political decision to transform these advantages into integrated public policy.

THE 5 SECTORS MOST VULNERABLE TO CYBERATTACKS IN GUATEMALA (ONE IS THE GOVERNMENT)

Prensa Libre – Recent cyberattacks against public institutions in Guatemala have once again highlighted the vulnerability of the country's technological infrastructure. In recent months, the General Directorate of Arms and Ammunition Control (Digecam) was the target of an incident in which information on firearm owners was stolen. Subsequently, the Ministry of Labor's (Mintrab) job portal, Tu Empleo, was also compromised, in addition to other incidents targeting state entities.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 10, 2026

A BILL HAS BEEN INTRODUCED TO STRENGTHEN CYBERSECURITY AND PROTECT THE DATA OF MENDOZA RESIDENTS - ARGENTINA

San Rafael Daily - The Mendoza government presented a cybersecurity bill to the provincial Senate aimed at strengthening the protection of the state's technological infrastructure and the personal data of Mendoza residents. The initiative seeks to establish a legal framework to prevent and respond to cyberattacks, while also ensuring the continuity of essential services such as security, health, education, transportation, and energy.

HOW CONNECTIVITY AND ARTIFICIAL INTELLIGENCE ARE TRANSFORMING BUSINESSES IN LATIN AMERICA

IT Site - Digital transformation is entering a new phase in Latin America. While in recent years the focus has been on adopting technological infrastructure and migrating to digital environments, today organizations are pursuing a much more ambitious goal: integrating technologies capable of generating efficiency, improving productivity, and delivering a measurable return on investment. In this scenario, connectivity, artificial intelligence (AI), cybersecurity, and critical infrastructure are no longer independent initiatives but have become components of a comprehensive strategy. Companies in sectors such as telecommunications, healthcare, education, industry, retail, and government are redefining their investment plans with the aim of building technological ecosystems prepared to respond to current and future business demands.

THE NEXT CYBERSECURITY CRISIS WON'T BE AN ATTACK. IT WILL BE A DECISION WE FAILED TO MAKE IN TIME.

Entrepreneur - There's a constant in the history of innovation: organizations rarely fail because a technology takes them by surprise. They almost always fail because they interpreted the first signs of change as issues too distant to alter the decisions they were making in the present. This happened with the internet when it still seemed like an academic experiment, it happened again with cloud computing, and more recently with artificial intelligence (AI). Today, everything indicates that we are facing a similar moment with quantum computing. Not because companies are unaware that it's coming, but because many remain convinced that they still have time to prepare.

RECORDED FUTURE ARRIVES IN COLOMBIA AMID HISTORIC SURGE IN CYBERATTACKS

Impactotic, a new cybersecurity and fraud prevention company, has announced its arrival in Colombia, promising to strengthen the defenses of public and private entities against an increasingly hostile digital environment. The Boston-based threat intelligence firm, with a presence in over 80 countries and specializing in sectors such as government, banking, and critical infrastructure, arrives amidst a historic surge in cybercrime.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 10, 2026

GOOGLE AND THE FBI TARGET MASSIVE BOTNET THAT QUIETLY USED HOME DEVICES TO MASK CYBERCRIME

CNET - The FBI, in partnership with Google and other tech companies, struck a massive blow against NetNut, a public-facing residential network proxy service that secretly hosted a botnet controlling approximately 2 million Android TVs and similar smart home devices. The network was being used for password-spraying, credential attacks and other malicious activity. Residential proxy botnets make malicious traffic appear like normal internet use, allowing everyday devices to be secretly hijacked by cybercriminals to conduct illegal activities using your home internet. Infected home devices were often preloaded with malicious software used by the botnet, which made traditional home security practices less effective at detecting and stopping the problem.

WHY THE WORLD NEEDS A CITIZENS' CYBERATTACK FRAMEWORK

WEF - When a major brand or piece of critical national infrastructure suffers a cyberattack, it makes national headlines. Governments convene, regulators act and the cybersecurity industry mobilizes. When a single parent is defrauded out of their savings, or a teenager's intimate images are shared without consent, the response is fractured, slow, and too often, non-existent. To many, it makes sense to prioritize these large attacks, but there is a bigger picture. Attacks against individuals are happening on a vast scale, and the cumulative impact, especially over the long term, is likely to be catastrophic for society. How are we going to run our economies and public services digitally when there is a loss of trust in interacting online?