DIGI AMERICAS ALLIANCE MEMBERS

Apple AppGate aws Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE
fluidattacks Google kriptos LUMU netskope paloalto NETWORKS Schneider Electric
SISAP Sistemas Aplicativos SOPHOS TANIUM tenable Trellix TrendAI whalemate zscaler

LAWMAKERS CALL FOR STRONGER DIGITAL SECURITY AMID RISE IN INTERNET FRAUD — MEXICO

Tecnoempresa - In order to prevent citizens from falling victim to fraud in the issuance of Mexican passports, the Permanent Commission of the Congress of the Union urged the Ministry of Foreign Affairs to strengthen its ongoing information campaign and cybersecurity measures for the application process. According to the report, passport-related cyber fraud is a persistent problem: citizens are deceived through fraudulent websites that impersonate the Ministry of Foreign Affairs, resulting in improper payments and the illicit collection of personal data, thus violating their right to identity and eroding trust in state institutions.

AMITI AND ALLIES LAUNCH THE "CYBERSECURE SMES" INITIATIVE TO PROTECT MEXICO'S ECONOMIC ENGINE

Edomex al Día - The Mexican Association of Information Technology Industries (AMITI), along with technology leaders such as Capa 8, KIO IT Services, and Mastercard, officially launched the national initiative "Cybersecure SMEs." The program aims to equip small and medium-sized enterprises with the capabilities, tools, and knowledge necessary to withstand, respond to, and recover from the growing digital threats.

THE FUTURE OF CYBERSECURITY IN PARTNERSHIP WITH THE LARGEST DIGITAL ECOSYSTEM — MEXICO

Boletin.mx - As connectivity grows, so does complexity. The international football tournament is witnessing an unprecedented moment: for the first time, a global event is bringing together more than 5 million people in person and billions more through digital platforms simultaneously. What is truly significant is what it represents: a large-scale demonstration of what major international events of the future will be like, with increasingly connected experiences driven by artificial intelligence and interdependent infrastructures.

THE CONGRESSIONAL ECONOMICS COMMITTEE MADE PROGRESS IN DEFINING CYBERSECURITY CRIMES – GUATEMALA

Infobae - The Economy Committee of Guatemala's Congress made progress this week in defining the crimes to be included in a future cybersecurity law, a pending requirement for the country to join the Budapest Convention before the extension expires in March 2027. The legislative team reviewed a comparative chart with three proposals and focused the debate on a list of eight criminal offenses: unauthorized access to systems or data, unauthorized interception, attacks on data and system integrity, computer forgery, computer fraud, misuse of devices, and child pornography. The most heated discussion centered on the proportionality of the penalties.

GUATEMALA AND THE U.S. DISCUSS BORDER SECURITY, DRUG TRAFFICKING, MIGRATION, AND ECONOMIC DEVELOPMENT

Prensa Libre – Guatemalan Ambassador to the United States, Hugo Beteta, held a meeting at the White House with high-ranking U.S. government officials to discuss security, the fight against drug trafficking, migration, and economic cooperation, the Ministry of Foreign Affairs reported. The Guatemalan delegation presented progress on joint border security efforts, migration coordination, and increased drug seizures, and discussed expanding cooperation with U.S. Southern Command. Beteta reiterated Guatemala's commitment to democratic governance, cybersecurity, and regional stability.

EL SALVADOR PRIORITIZES DIGITAL CONNECTIVITY, TRANSPORTATION, AND ENERGY IN THE NEW POLITICAL PHASE WITH THE EUROPEAN UNION

Infobae – El Salvador, the European Union, and Central America launched a new phase of joint political work in Brussels with the first meeting of the Political Pillar Committee of the Association Agreement, focusing on digital connectivity, transportation, and energy to expand regional cooperation. The Salvadoran delegation, led by Vice Minister Adriana Mira, highlighted the implementation of the Regional Digital Strategy, which has strengthened e-government frameworks, the digitization of public services, cybersecurity, and interoperability among Central American countries.

PANAMA WILL LAUNCH ITS NATIONAL ARTIFICIAL INTELLIGENCE STRATEGY ON JULY 30

Telemetro - Panama will take a step toward strengthening its technological development with the launch of the National Artificial Intelligence Strategy and the National Semiconductor and Microelectronics Strategy, scheduled for July 30. The announcement was made by the National Secretary of SENACYT (National Secretariat of Science, Technology and Innovation), Eduardo Ortega, who highlighted that the event will bring together representatives from renowned universities and companies in the technology sector. The National Artificial Intelligence Strategy seeks to promote the responsible use of this technology in various sectors.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 16, 2026

CISA AND PARTNERS PUBLISH GUIDANCE TO HELP SOFTWARE MANUFACTURERS AND ONLINE SERVICE PROVIDERS WORK WITH SECURITY RESEARCHERS — USA

CISA - CISA, the National Security Agency and international partners published joint guidance urging software manufacturers and online service providers to build formal coordinated vulnerability disclosure (CVD) programs rather than rely on improvised email exchanges when researchers find security flaws. The document covers the full operational chain: receiving reports, communicating with researchers, triaging findings, developing fixes, coordinating disclosure and assigning CVE identifiers. It also recognizes that smaller or less mature vendors may need CISA or another national CSIRT to act as an intermediary, and fits within CISA's broader Secure by Design initiative.

US LAUNCHES VULNERABILITY CLEARINGHOUSE AMID AI-FUELED SURGE IN FLAWS

Cybersecurity Dive - The Trump administration announced the launch of Gold Eagle, a program that will coordinate the security community's use of frontier AI models to rapidly identify and fix vulnerabilities. The clearinghouse responds to the skyrocketing number of vulnerabilities AI models are finding and the strain that surge places on defenders; through it, the government will coordinate private companies and independent researchers to scan critical software packages, fix flaws and deploy those fixes. The core of the program is the Vulnerability Information and Coordination Environment (VINCE), operated with Carnegie Mellon's Software Engineering Institute, with a heavy focus on open-source software.

THREE RUSSIAN NATIONALS AND TWO COMPANIES INDICTED FOR INTERNATIONAL CYBERCRIMES RESULTING IN MORE THAN $62M IN VICTIM LOSSES

U.S. Department of Justice - An indictment was unsealed in the Northern District of Ohio charging three Russian nationals and two related "bulletproof hosting" companies, Medialand LLC and ML.Cloud LLC, for their roles in cybercrimes against U.S. victims that caused tens of millions of dollars in losses. According to court documents, the St. Petersburg-based firms leased infrastructure to cybercriminals to infect victims with malware and ransomware, support criminal marketplaces, register fraudulent domains and launch phishing and brute-force attacks. The indictment alleges 42 victims across 21 states — including banks, schools, hospitals, government entities and media companies — were targeted.

THREE LESSONS ON CYBERSECURITY AND DIGITAL RISK FROM THE WORLD CUP

WEF - Most organizations now operate in the same basic conditions that define a World Cup: fixed deadlines, high-value data, customer-facing systems, connected suppliers and very little tolerance for downtime. A retailer preparing for Black Friday, a bank handling market volatility or a hospital managing patient flow all face the same question: can the business keep operating when its digital systems come under pressure? At the World Cup, all those things are simply bigger, faster, more public and compounded by geopolitics.