DIGI AMERICAS ALLIANCE MEMBERS

Apple aws Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks
Google kriptos LUMU netskope paloalto NETWORKS Resecurity
Schneider Electric SISAP Sistemas Aplicativos Strike Telefónica tenable Trellix TREND MICRO

MEXICO AND THE REPUBLIC OF ESTONIA WILL SEEK EXCHANGES ON GOVERNMENT DIGITIZATION AND CYBERSECURITY

Talla Politica - At the inauguration of the Mexico-Estonia Friendship Group, its president, Representative Deliamaria González Flandez (PVEM), stated that its purpose will be to foster exchange in the areas of government digitalization, cybersecurity, technological training, and e-commerce. The legislator indicated that the relationship between the two nations is based on shared values and a common vision for the future. “Mexico, as a diverse nation with a strategic role in the region, and Estonia, as a leader in digitalization, e-government, and innovation, have built a binational dialogue based on respect and cooperation.”

THE DOMINICAN REPUBLIC ASSUMES THE 2026 PRESIDENCY OF THE GEALC NETWORK

Presidencia.gob.do - The Dominican Republic was elected to the Executive Committee and will assume the 2026 Presidency of the Inter-American Digital Government Network (Red GEALC). The announcement was made during the 19th Annual Meeting of Red GEALC, held in Guatemala, where the Government Office of Information and Communication Technologies (OGTIC) represented the country. Reyson Lizardo, Director of Government Digital Transformation at OGTIC, stated from there: “This achievement reaffirms the Dominican Republic’s commitment to innovation, transparency, and efficiency in government, and consolidates our role as a leader in digital government in Latin America and the Caribbean.”

EXTORTION IN THE HEALTHCARE SECTOR TRIPLES AND 88 CYBERCRIMINAL GROUPS THREATEN THE INDUSTRY - CHILE

TrendTIC - The healthcare sector faces a new phase of cybersecurity risk. According to the report "State of Ransomware in the Healthcare Sector 2025," prepared by cybersecurity experts, extortion based solely on data theft —without the need to encrypt or block it—has tripled since 2023, becoming the most aggressive and fastest-growing type of cyberattack among all the economic sectors analyzed in the study.

LULA DA SILVA CRITICIZES TECHNOLOGICAL CONCENTRATION AT THE G20 AND CALLS FOR AI GOVERNANCE - BRAZIL

DPL News – During his speech at the G20 Summit in Johannesburg, Brazilian President Luiz Inácio Lula da Silva reiterated his criticism of the global concentration of technology and advocated for greater digital autonomy for developing countries. The president stated that the control of data, algorithms, and infrastructure by large economies exacerbates inequalities and can lead to “digital colonialism.”

TRENDS FOR THE ELECTRONIC SECURITY MARKET IN BRAZIL IN 2026

Revista Seguranca Eletronica - The electronic security market in Brazil is consolidating itself as one of the most dynamic in Latin America, projected to reach a revenue of over R$ 18 billion in 2026, driven by a compound annual growth rate (CAGR) of approximately 12% from the R$ 14 billion recorded in 2024.

THE IBERO-AMERICAN CYBER DEFENSE FORUM MEETS IN MADRID

Segurilatam - Madrid hosted the 8th Ibero-American Cyber Defense Forum on November 26th. Spain, as the holder of the Pro Tempore Secretariat, hosted this meeting, which coincided with the STIC Conference organized by the Spanish National Cryptologic Center and the Joint Cyber Command. Major General Gómez Lera presided over what was the Forum's first in-person meeting.

ADAPTING TO THE CONSUMER, THE KEY STEP TO DIGITIZING SMES IN THE REGION

Revista E&N - How can we help SMEs take a leap in digital transformation? From Miami, the Mastercard Innovation Forum proposes a roadmap for the region's small and medium-sized enterprises, which account for 75% of global employment. While there is no single solution due to the unique characteristics of each company, the proposal is for SMEs to adapt to their customers' consumption habits and adopt a full range of digital payment options. The idea is to support business owners in building, growing, and protecting their companies in an increasingly digital economy.

ALMOST 1 BILLION ATTEMPTS TO ACCESS MALICIOUS SITES BLOCKED BY NEW GOVERNMENT CYBER TOOL - UNITED KINGDOM

NCSC - Almost one billion early-stage cyber attacks and attempts to access scam websites have been blocked by a new government cyber service in less than a year, according to new figures from GCHQ’s National Cyber Security Centre (NCSC) and BT. The Share and Defend service – developed by experts at NCSC – works to disrupt online crime by sharing near real-time data on known fraudulent and malicious websites with internet service providers, which can then prevent customers from clicking through.

NSA, CISA, AND OTHERS RELEASE GUIDANCE ON INTEGRATING AI IN OPERATIONAL TECHNOLOGY - USA

NSA - The National Security Agency (NSA) is joining the Cybersecurity and Infrastructure Security Agency (CISA), the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), and others in releasing the Cybersecurity Information Sheet (CSI), "Principles for the Secure Integration of Artificial Intelligence in Operational Technology." While artificial intelligence (AI) presents potential to enhance efficiency, productivity, decision-making, and customer experiences, adopting AI into operational technology (OT) systems introduces new risks to the safety and security of the environments they are integrated in and critical functions they support.

AISURU BOTNET BEHIND NEW RECORD-BREAKING 29.7 TBPS DDOS ATTACK

Bleeping Computer - In just three months, the massive Aisuru botnet launched more than 1,300 distributed denial-of-service attacks, one of them setting a new record with a peak at 29.7 terabits per second. Aisuru is a huge botnet-for-hire service that provides an army of routers and IoT devices compromised via known vulnerabilities or through brute-forcing weak credentials. Internet management and infrastructure company Cloudflare estimates that the botnet uses between one and four million infected hosts across the world.

A DECADE OF RANSOMWARE CHAOS – HOW MUCH IT COSTS

Cybersecurity Ventures - IoT for all reports that over the past decade, ransomware has evolved from a small-scale threat targeting personal computers into a systemic risk affecting critical infrastructure, smart factories, and connected devices. In 2015, the FBI received approximately 2,400 ransomware complaints, resulting in losses exceeding $24 million. That same year, broader estimates put ransomware damage at around $300 million. By 2017, the scale had expanded, and damage estimates had risen to $5 billion. Fast forward to 2021, ransomware damages to organizations were estimated at $20 billion, according to Cybersecurity Ventures, with attacks occurring roughly every 11 seconds.

FIGHTING CYBER-ENABLED FRAUD: A SYSTEMIC DEFENCE APPROACH

WEF - Phishing and cyber-enabled fraud are escalating global threats affecting users, consumers, organizations and countries alike. This white paper, Fighting Cyber-Enabled Fraud: A Systemic Defence Approach, developed by the World Economic Forum's Partnership against Cybercrime in collaboration with the Institute for Security and Technology, presents a systemic defence framework to confront this challenge. Turning the tide on cyber-enabled fraud demands a truly systemic approach, one that maximizes the impact of upstream interventions while ensuring broad, consistent coverage through downstream measures, and this paper calls on stakeholders to act across three complementary pillars of systemic defence: Prevention, Protection and Mitigation. It also demonstrates how a multistakeholder, upstream-focused model can shift responsibility to those best positioned to act at scale, empowering them to prevent harm before it takes root.