DIGI AMERICAS ALLIANCE MEMBERS

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

THE DOMINICAN REPUBLIC HOSTS AN INTERNATIONAL EVENT ON CYBERSECURITY AND CYBER DIPLOMACY

Presidency of the Dominican Republic - The Dominican Republic is hosting, for the first time, the “Tallinn Cyber Diplomacy Winter School 2025,” a prominent international event that seeks to strengthen international cooperation in cybersecurity and promote capacity building in cyber diplomacy. For three days, the Indotel Cultural Center, home to the Latin American and Caribbean Cybercapabilities Center (LAC4), will become the global meeting point for cybersecurity and digital diplomacy, bringing together experts, diplomats, and academics from around the world.

GOVERNMENT STRENGTHENS CYBERSECURITY CAPABILITIES TO COMBAT DIGITAL THREATS - GUATEMALA

Ministry of the Interior - As part of the program to strengthen capacities against digital threats, a major cybersecurity training session was held for public administration officials. The training, led by experts in the field from Colombia, took place on March 11 in the Main Hall of the Ministry of the Interior, Zone 1 of the capital. In his speech, the Deputy Minister of Information and Communications Technology, William Cameros, highlighted the importance of cybersecurity training in public administration.

AGENCIES MUST GUARANTEE DATA CONFIDENTIALITY WHEN CONTRACTING CLOUD USE FOR CREDIT HISTORY, ACCORDING TO THE BCR AND SSF - EL SALVADOR

El Mundo - The hiring of cloud computing to store credit information for financial system users in El Salvador must guarantee data confidentiality, warns the Central Reserve Bank (BCR) in a study of the reform to the Credit History Law. Representatives of the Central Reserve Bank (BCR) and the Superintendency of the Financial System (SSF) warned legislators this Friday that the hiring of cloud computing to store credit information for financial system clients in El Salvador must guarantee cybersecurity mechanisms and data confidentiality.

THE OBLIGATION TO REPORT CYBERSECURITY INCIDENTS COMES INTO FORCE - CHILE

PubliMetro - On February 28 and March 1, two regulations were published in the Official Gazette that complement the cybersecurity framework law. These regulations require public and private institutions—considered essential service providers and operators of vital importance—to report their cyber incidents to the National CSIRT (Computer Security Incident Response Team). They establish that an incident is considered "significant" when it interrupts an essential service, affects the physical integrity or health of individuals, compromises the confidentiality or integrity of IT assets, allows unauthorized access to computer networks or systems, and/or affects systems containing personal data.

BIOMETRIC AUTHENTICATION: A SOLUTION IN CHILE FOR PROTECTING DIGITAL DATA

Portal Innova - The digital fraud landscape in Chile is becoming increasingly complex. The increasing digitalization of transactions, coupled with the growing sophistication of cybercriminals, demands more robust and efficient security measures. In this scenario, digital identity validation and biometric authentication are positioned as fundamental elements to protect users and their data, as the industry moves toward a "passwordless" future, abandoning traditional passwords in favor of more secure and convenient methods.

COLOMBIA | CYBERSECURITY: INTEGRATING BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE TO STRENGTHEN DIGITAL PROTECTION

dplnews - Over the last decade, Colombia has undergone a significant digital transformation that has boosted the country's economic and social development. However, this progress has also brought with it an increase in cyber threats, leading to greater concerns about cybersecurity, information protection, and cybersecurity in general. In this context, emerging technologies such as blockchain and artificial intelligence (AI) are emerging as key tools to strengthen defenses against cyberattacks and ensure the integrity of the country's data.

THE GROWTH OF BUG BOUNTY IN BRAZIL: THE NEW FRONTIER OF CYBERSECURITY

inforchannel - Digital security is no longer a topic restricted to large corporations and has become a real concern for companies in all sectors. The rapid growth of cyber attacks, combined with Digital Transformation and the advancement of Data protection regulations, has driven a new protection model that is already widely adopted by large international corporations: Bug Bounty.

BRAZIL'S COMDCIBER STANDS OUT IN CYBER WARFARE EXERCISE WITH 26 COUNTRIES

Convergencia DIgital - The Cyber Defense Command (ComDCiber) represented Brazil in Defense Cyber Marvel 4 (DCM4), one of the largest cybersecurity exercises in the world, coordinated by the United Kingdom Army, which involved 26 countries with remote participation from 20 locations, with its main headquarters in Seoul, South Korea. According to General Ivan de Sousa Corrêa Filho, executive secretary of the Institutional Security Office and future commander of ComDCiber, the Brazilian team performed at a high level. “We were very pleased,” he told Convergência Digital.

OAS SEEKS TO MEASURE MATURITY OF RESPONSE TO CYBER INCIDENTS

dplnews - The Organization of American States (OAS) presented the "CSIRT Americas Baseline" guidelines, aimed at measuring the maturity of Cyber Incident Response Teams (CSIRTs). These guidelines, the OAS stated, act as drivers for the Cybersecurity Section of the Inter-American Committee against Terrorism (CICTE) in strengthening the region's cyber incident response capabilities.

ARE SATELLITES CRITICAL INFRASTRUCTURE?

SEGURILATAM - Typically, when referring to critical infrastructure that provides essential services, people think of power plants, hospitals, airports, etc. However, aerospace infrastructure is often relegated to the background. Among them are satellites, which play a fundamental role in providing services such as communications, navigation, earth observation, and meteorology. Therefore, they must be considered critical infrastructure that, like terrestrial infrastructure, requires both physical and cyber protection.

NIST RELEASES DRAFT CYBERSECURITY WHITE PAPER ON CRYPTO AGILITY, AIMS TO SHAPE FUTURE CYBERSECURITY STRATEGIES - USA

Industrial Cyber - The U.S. National Institute of Standards and Technology (NIST) released an initial public draft of a Cybersecurity White Paper. This document offers a comprehensive analysis of current strategies for achieving crypto agility. It explores the challenges and trade-offs involved and outlines methods for implementing operational mechanisms that ensure crypto agility while preserving interoperability. Additionally, it emphasizes key areas that need further discussion.

AI ENHANCES SECURITY AND PUSHES PRIVACY BOUNDARIES

Forbes - Artificial Intelligence is reshaping cybersecurity and digital privacy, promising enhanced security while simultaneously raising questions about surveillance, data misuse, and ethical boundaries. As AI-driven systems become more embedded in daily life—from facial recognition software to predictive crime prevention—consumers are left wondering: where do we draw the line between protection and overreach? The same AI technologies that help identify cyber threats, streamline security operations, and prevent fraud are also capable of mass surveillance, behavioral tracking, and intrusive data collection. In recent years, AI-powered surveillance has come under scrutiny for its role in government tracking, corporate data mining, and law enforcement profiling. Without clear regulations and transparency, AI risks eroding fundamental rights rather than protecting them.

THE AI CYBERCRIME WAVE HAS NOW REACHED 87% OF GLOBAL BUSINESSES

The CFO - A new arms race is unfolding in cybersecurity, and artificial intelligence is at its core. Attackers are using AI to supercharge deception, making fraud more convincing, more scalable, and harder to detect. The numbers are staggering: 87% of global organizations faced an AI-powered cyberattack in the past year, according to SoSafe's Cybercrime Trends 2025 report. And the threat is only accelerating.

BALANCING CYBERSECURITY ACCOUNTABILITY & DEREGULATION

Dark Reading - As the US transitions into a new administration, deregulation — or perhaps even outright abolishing certain agencies and functions — is set to be a defining theme of 2025. While federal agencies across sectors like labor, education, and transportation are expected to be slashed in an effort to cut red tape and fuel economic growth, cybersecurity regulations will be consolidated within agencies like the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Administration (CISA). Simultaneously, they will tighten regulations to protect national security.