DIGI AMERICAS ALLIANCE MEMBERS

PANAMÁ ANTE 5G: EL RETO DE CONSTRUIR UNA REGULACIÓN DE CIBERSEGURIDAD PARA INFRAESTRUCTURAS CRÍTICAS

La Estrella de Panama - Ante el próximo despliegue de la tecnología 5G, expertos advierten que Panamá aún carece de un marco integral de ciberseguridad para proteger infraestructuras críticas y redes de telecomunicaciones. La experiencia de regiones como la Unión Europea, Estados Unidos y Costa Rica muestra la importancia de establecer normas que fortalezcan la seguridad digital, la confianza de los usuarios y la resiliencia de servicios estratégicos.

EEUU ENTREGA A PANAMÁ EQUIPOS DE SEGURIDAD MARÍTIMA, FRONTERIZA Y CIBERNÉTICA

La Tribuna - La embajada de EE.UU. informó este miércoles que entregó al Gobierno de Panamá «equipos esenciales de seguridad marítima, fronteriza y cibernética» por valor de cinco millones de dólares, como parte de la cooperación para desarticular las redes que impulsan la migración irregular y el narcotráfico y fortalecer la protección del Canal interoceánico. «Este apoyo forma parte de la cooperación ampliada en seguridad del Comando Sur de EE.UU. a Panamá, que en 2026 alcanzará un valor estimado de 100 millones de dólares», indicó la embajada estadounidense en un comunicado.

GOBIERNO NACIONAL ACTIVA PMU CIBERNÉTICO PARA PROTEGER LA SEGUNDA VUELTA ELECTORAL - COLOMBIA

ImpactoTIC - Con el objetivo de salvaguardar el entorno digital y fortalecer la confianza ciudadana de cara a la segunda vuelta presidencial del próximo 21 de junio, el Ministerio TIC anunció la activación del Puesto de Mando Unificado (PMU) Cibernético. La estrategia busca coordinar acciones de monitoreo, prevención y respuesta frente a incidentes de ciberseguridad que puedan afectar el desarrollo normal de la jornada democrática. El PMU Cibernético no es una iniciativa nueva. Fue instalado oficialmente el 8 de marzo de 2026 para acompañar las elecciones legislativas y desde entonces funciona como un mecanismo de articulación interinstitucional entre entidades responsables de la seguridad digital, la defensa y la organización electoral.

EL G7 TRABAJARÁ PARA QUE LOS MODELOS DE IA NO CAIGAN EN MANOS DE REGÍMENES AUTORITARIOS

infobae - El G7 ha lanzado un trabajo en común para una regulación de los modelos avanzados de la inteligencia artificial (IA) a fin de evitar las amenazas que pueden plantear en términos de ciberseguridad o para la sociedad, pero también para que no caigan en manos de regímenes autoritarios. El presidente francés, Emmanuel Macron, explicó al término de la cumbre del G7 de Évian, que concluyó con un almuerzo de los líderes de los siete países más ricos con una docena de dirigentes de empresas tecnológicas, que la idea es construir en los próximos meses "una plataforma de discusión y de cooperación entre democracias frente al riesgo de la inteligencia artificial".

LOS DRONES Y LA CIBERSEGURIDAD: EL INFORME QUE ALERTA AL MUNDIAL 2026 Y SUS HINCHAS

redgol - as medidas de seguridad se han extremado en el **Mundial 2026**, que se desarrolla en Canadá, Estados Unidos y México, siendo un foco que alarma a las autoridades. Por ejemplo, el FBI decidió poner tolerancia cero a los drones en los estadios donde se juegan los partidos, con prohibición de acercarse a los reductos, además donde están los hinchas. Mientras que en México el Grupo Especial Antidrones, alertados por la Guardia Nacional del país, dieron de baja un aparato que se acercó al lugar de entrenamiento de la delegación de la **selección de Corea del Sur**, aunque no lograron encontrar a los responsables. “Antes de que llegara el equipo nacional, dos hombres extranjeros sospechosos de ser los operadores huyeron con el dron”, detallaron.

ASÍ AVANZAN LOS PAÍSES DE AMÉRICA LATINA CON LOS COMPROMISOS DE LA CONFERENCIA MUNDIAL DE TELECOMUNICACIONES 2025

dpl News - Representantes de México, Guatemala, Honduras, Panamá y Trinidad y Tobago reunidos en el Foro Regional de Desarrollo para las Américas 2026 (ITURDF2026) expusieron las acciones que están implementando para dar continuidad a los compromisos adoptados durante la Conferencia Mundial de Desarrollo de las Telecomunicaciones 2025 (WTDC-25). Los panelistas destacaron que América Latina está traduciendo los compromisos adoptados en la WTDC-25 en acciones concretas relacionadas con conectividad, modernización regulatoria, gestión del espectro, ciberseguridad e Inteligencia Artificial (IA); no obstante, los desafíos persisten, especialmente en zonas rurales y poblaciones históricamente excluidas. Además, coincidieron en la necesidad de coordinar esfuerzos para acelerar la inclusión digital y aprovechar las oportunidades que ofrecen las nuevas tecnologías.

BRAZIL’S MATURING MARKET MEETS MATURING THREATS: HOW GLOBAL CRYPTO CRIME TRENDS ARE LANDING IN LATIN AMERICA’S LARGEST MARKET

Chainalysis - Brazil is Latin America’s largest crypto market, and one of the world’s most dynamic. Between July 2024 and June 2025, the country received an estimated $318 billion in on-chain value, roughly one-third of all cryptocurrency value received across Latin America. A large, relatively young population, a vibrant fintech sector that has normalized digital financial services for millions, and persistent demand for dollar-pegged stablecoins as an inflation hedge have all fueled that growth. But when a legitimate market grows at such a pace, it draws attention from illicit actors, too. Our data shows that’s exactly what’s happening. The same criminal networks dominating crypto laundering activity worldwide — Chinese-language money laundering networks (CMLNs), Russian sanctions evaders, and drug traffickers — have found a significant foothold in Brazil’s exchanges, according to our data.

WHITE HOUSE ROLLS OUT NSPM-12 TO BOOST CYBERSECURITY GOVERNANCE, OVERSIGHT, ACCOUNTABILITY FOR NATIONAL SECURITY SYSTEMS - USA

Industrial Cyber - The White House issued National Security Presidential Memorandum 12 (NSPM-12), establishing a new cybersecurity governance framework for National Security Systems (NSS), including military, intelligence, and other federal systems that process classified information. The memorandum re-establishes the Committee on National Security Systems (CNSS), a decades-old interagency body, designates the National Security Agency as the National Manager for NSS cybersecurity with expanded authority to assess security posture, issue emergency directives, and coordinate government-wide cyber defense activities.

OT SECURITY MATURITY IMPROVES ACROSS LATIN AMERICA

Mexico Business News - Organizations across Latin America are improving OT cybersecurity governance, visibility, and compliance readiness. However, cyber threats targeting industrial environments continue to evolve, keeping operational risk at elevated levels. The report suggests that organizations are becoming more realistic about their cybersecurity capabilities while recognizing that visibility, segmentation, remote access security, incident response, and architecture standardization remain critical areas requiring investment. This shift reflects a broader market transition in which OT security is increasingly linked to executive oversight, regulatory compliance, and operational resilience.

CYBERCRIME IS CONVERGING. THE RESPONSE MUST CONVERGE FASTER

WEF - Cybercrime is evolving into a converged criminal economy that connects online fraud, ransomware, extortion, money laundering, human trafficking, organized crime and, in some cases, state-aligned activity.
This convergence changes the nature of the threat. Criminal groups are not merely adopting new tools. They are combining capabilities, sharing infrastructure and building operating models that span technical, geographic and jurisdictional boundaries. The same ecosystem that supports credential theft or ransomware can also fund scam compounds, exploit trafficked labor, move illicit proceeds and goods and enable broader organized crime.

AI, QUANTUM AND THE NEW CYBERSECURITY FRAMEWORK IMPERATIVE

Forbes - With developing technologies, cybersecurity, and risk, one theme has been consistent: technical innovation continues to outpace our ability to safeguard it. Today's organizations face a defining problem. They must work in a world where artificial intelligence, quantum computing, cloud services, edge computing, IoT, sophisticated telecommunications, and digital ecosystems increasingly intertwine. The consequent prospects are remarkable. The risks are as significant. The cybersecurity discussion must be limited to attack prevention. The true task for this year and beyond is to strengthen organizational resilience and promote trust in an increasingly interconnected society. The digital economy now relies on trust as its currency. Customers entrust firms with their personal information. Citizens trust their governments to protect key services. Businesses rely on global supply chains, cloud providers, and digital platforms to support critical operations.