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 SOPHOS tenable Trellix TrendAI whalemate

PRESENTAN INICIATIVA ANTE AUMENTO DE ATAQUES CIBERNÉTICOS - GUATEMALA

Congreso.gob.gt - Ante los ataques cibernéticos registrados en las últimas semanas a distintas entidades estatales, lo diputados del bloque Viva, entre ellos el parlamentario Gerson Barragán, Tercer Secretario de la Junta Directiva; Edin de Jesús y Obbed Castañasa, jefe y subjefe de la bancada respectivamente, presentaron este martes una iniciativa de ley que busca crear el sistema nacional de ciberseguridad. En conferencia de prensa, el jefe del bloque explicó que la propuesta contiene 76 artículos orientados a establecer un marco jurídico integral para la prevención, gestión y respuesta ante riesgos informáticos que afectan servicios públicos y datos personales de los ciudadanos.

IMPULSAN LEY DE CIBERSEGURIDAD EN HONDURAS; ¿DE QUÉ SE TRATA?

Tiempo - El diputado por el Partido Liberal, José Rolando Sabillón, informó que busca impulsar una Ley de Ciberseguridad para que sea incluida en el paquete de reformas al Código Penal que está próximo a discutirse en el Congreso Nacional. Sabillón señaló que el país enfrenta un rezago significativo en esta materia y carece de una legislación base que permita estructurar un sistema nacional de ciberseguridad. Según explicó, actualmente Honduras no cuenta con una normativa integral que sirva como fundamento para enfrentar los delitos tecnológicos. “Estamos en pañales en los temas de ciberseguridad. No tenemos una ley que sirva como cimiento, como base sólida para enfrentar estos delitos”, expresó el congresista.

DECEA, DA FORÇA AÉREA BRASILEIRA, DEBATE SATÉLITES E DEFESA CIBERNÉTICA NA AVIAÇÃO E INDICA MEDIDAS PARA SEGURANÇA DO TRÁFEGO AÉREO

Defesa TV - Em 4 de maio, o Departamento de Controle do Espaço Aéreo, órgão da Força Aérea Brasileira, reuniu especialistas do SISCEAB para um debate estratégico sobre uso de satélites e defesa cibernética na aviação.
A pauta evidenciou a evolução das telecomunicações aeronáuticas, com expansão de SATCOM e comunicações por radiofrequência, além do conceito D2D, elevando a resiliência e a continuidade dos serviços.

DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 7, 2026

CASI 15 MILLONES DE DATOS DE IDENTIDAD DE ECUATORIANOS APARECIERON EN REDES Y FOROS CLANDESTINOS: AUTORIDADES INVESTIGAN UNA NUEVA FILTRACIÓN MASIVA

infobae - Una nueva alerta de ciberseguridad sacudió a Ecuador esta semana después de que plataformas especializadas detectaran la supuesta filtración de casi 15 millones de registros de identidad de ciudadanos ecuatorianos en foros clandestinos y redes sociales. La información expuesta incluiría nombres completos, números de cédula, fotografías tipo carnet, firmas y datos biométricos asociados al sistema de identificación nacional.

POLICÍA CIBERNÉTICA REFUERZA ACCIONES CONTRA EL FRAUDE ELECTRÓNICO EN EL EDOMEX: ESTAS SON LAS RECOMENDACIONES - MÉXICO

infobae - La Policía Cibernética del Estado de México reforzó medidas para combatir el fraude electrónico ante el aumento de reportes ligados a compras y ventas en línea. Mediante un comunicado en sus canales oficiales, la Secretaría de Seguridad estatal (SSEM) advirtió que el uso extendido de plataformas digitales, redes sociales y aplicaciones de mensajería facilitó modalidades de engaño que afectan a la población mexiquense. La dependencia recomendó fortalecer hábitos de prevención y canalización de denuncias para reducir riesgos en transacciones electrónicas.

CIBERSEGURIDAD: LA NUEVA DEFENSA EN TIEMPOS DIGITALES - MÉXICO

Cronica - En un mundo cada vez más interconectado, los ataques digitales se han convertido en una de las principales amenazas para empresas, instituciones públicas y organizaciones de todos los tamaños. Robo de datos, secuestro de información y fraudes electrónicos son riesgos cotidianos que han detonado una creciente demanda de especialistas capaces de anticipar, detectar y neutralizar amenazas. En respuesta, el Laboratorio de Redes y Ciberseguridad Cisco de la Universidad Autónoma de Guadalajara (UAG) se consolida como un espacio estratégico para la formación de “guardianes digitales”. Respaldado por el programa global Cisco Networking Academy, este centro permite a los estudiantes adquirir competencias en configuración de redes, análisis de vulnerabilidades, gestión de incidentes y diseño de arquitecturas seguras, además de prepararse para certificaciones internacionales que fortalecen su perfil profesional.

ADIÓS A LAS CONTRASEÑAS TRADICIONALES: ASÍ AVANZA LA NUEVA ERA DE LA CIBERSEGURIDAD DIGITAL

infobae - El modelo tradicional de contraseñas está quedando atrás. En un sistema donde más del 90% de los incidentes de seguridad tienen su origen en credenciales débiles, robadas o reutilizadas, expertos y organizaciones advierten que la industria avanza hacia sistemas de autenticación más seguros. La tendencia se consolida en el marco del Día Mundial de la Contraseña, impulsada por el aumento de ataques como el phishing personalizado y el “credential stuffing”, que explotan vulnerabilidades en el uso de claves tradicionales.

DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 7, 2026

CISA TELLS CRITICAL ORGANIZATIONS TO PREPARE FOR CYBER OUTAGES - USA

Federal News Network - CISA's new "CI Fortify" initiative notably pushes water utilities, the transportation sector and other critical infrastructure organizations to plan for a "geopolitical crisis" involving cyber attacks that could sever their connections to internet, telecommunications and other technology services. CISA's guidance features two primary emergency planning objectives: "isolation" and "recovery" to mitigate threats. The former involves "proactively disconnecting from third-party and business networks" to safeguard operational technology, such as industrial control systems, from cyber attack during a crisis. CISA says organizations should be prepared to sustain "essential operations" rather than completely shutting down.

NIST WILL TEST THREE MAJOR TECH FIRMS' FRONTIER AI MODELS FOR CYBERSECURITY RISKS - USA

Cybersecurity Dive - The U.S. government's AI security center will evaluate frontier models from Google, Microsoft and xAI before their release to determine whether the models' advanced capabilities pose cybersecurity risks. The newly announced plan for the National Institute of Standards and Technology's (NIST) Center for AI Standards and Innovation (CAISI) to conduct "pre-deployment evaluations" represents the U.S. government's most significant attempt yet to get ahead of security threats from powerful AI systems. "Independent, rigorous measurement science is essential to understanding frontier AI and its national security implications," CAISI Director Chris Fall said in a statement. "These expanded industry collaborations help us scale our work in the public interest at a critical moment."

EMPOWERING DEFENDERS: AI FOR CYBERSECURITY

WEF - AI is transforming cybersecurity, but realizing its full value requires strategic deployment, robust governance and balanced human oversight. This white paper, Empowering Defenders: AI for Cybersecurity, offers practical guidance for organizations seeking to harness AI in their cybersecurity efforts. To support effective implementation, the paper outlines the critical questions executives and chief information security officers must address and provides an early perspective on the opportunities and challenges posed by agentic AI. It suggests that executive and cyber leaders embarking on the AI adoption journey for cyber defence should: align the adoption of AI in cybersecurity with enterprise strategic priorities; establish organizational readiness across processes, data, infrastructure, skills and governance before deploying AI in cybersecurity; validate AI solutions through structured pilots prior to full deployment; and scale and monitor the performance of AI in cybersecurity and optimize as needed.

TARGET-RICH, CYBER-POOR: HOW TO STRENGTHEN CYBERSECURITY AND BUILD RESILIENCE IN VULNERABLE SECTORS

WEF - In June 2025, cyberattacks on two hospitals in north Delhi severely disrupted access to digital patient records, forcing staff to activate manual systems for patient care to maintain services during the incident. In September that same year, a ransomware attack on UK-based early childhood education provider Kido International exposed sensitive data of around 8,000 children and staff, including names and photographs. Both breaches triggered national cybersecurity warnings and led to the arrests of the perpetrators, underscoring the real-world risks cyberattacks pose to vulnerable communities. The World Economic Forum's Global Cybersecurity Outlook 2025 highlighted that the growing complexity of cyberspace is exacerbating cyber inequity, widening the gap between sectors.