DIGI AMERICAS ALLIANCE MEMBERS

LA REPÚBLICA DOMINICANA ES SEDE DE EVENTO INTERNACIONAL SOBRE CIBERSEGURIDAD Y DIPLOMACIA CIBERNÉTICA

Presidencia de la Republica Dominicana - La República Dominicana es sede, por primera vez, del “Tallinn Cyber Diplomacy Winter School 2025”, un destacado evento internacional que busca fortalecer la cooperación internacional en ciberseguridad y promover la construcción de capacidades en la diplomacia cibernética. Durante tres días, el Centro Cultural Indotel, donde se encuentra ubicado el Centro de Cibercapacidades de Latinoamérica y el Caribe (LAC4), se convierte en el punto de encuentro global para la ciberseguridad y la diplomacia digital, reuniendo a expertos, diplomáticos y académicos de todo el mundo.

GOBERNACIÓN FORTALECE CAPACIDADES EN CIBERSEGURIDAD ANTE AMENAZAS DIGITALES - GUATEMALA

Ministerio de Gobernacion - Como parte del programa de fortalecimiento de capacidades ante amenazas digitales, se desarrolló una importante capacitación en ciberseguridad dirigida a funcionarios de la administración pública. La formación, dirigida por expertos en la materia proveniente de Colombia, se realizó este 11 de marzo en el Salón Mayor de la Cartera del Interior, zona 1 capitalina.El Viceministro de Tecnología de la Información y las Comunicaciones, William Cameros, en su intervención, destacó la importancia de la formación en ciberseguridad en la gestión pública.

AGENCIAS DEBERÁN GARANTIZAR CONFIDENCIALIDAD DE DATOS AL CONTRATAR USO DE NUBE PARA HISTORIAL CREDITICIO SEGÚN BCR Y SSF - EL SALVADOR

El Mundo - La contratación de nube para guardar la información crediticia de usuarios del sistema financiero en El Salvador deberá garantizar la confidencialidad de los datos, advierte el Banco Central de Reserva en estudio de reforma a Ley del historial crediticio. Representantes del Banco Central de Reserva (BCR) y de la Superintendencia del Sistema Financiero (SSF) advirtieron este viernes a los diputados que la contratación de la nube para el resguardo de información crediticia de los clientes del sistema financiero en El Salvador deberá garantizar mecanismos de ciberseguridad y confidencialidad de los datos.

ENTRA EN VIGOR LA OBLIGACIÓN DE REPORTAR INCIDENTES DE CIBERSEGURIDAD - CHILE

PubliMetro - El 28 de febrero y el 1 de marzo fueron publicadas en el Diario Oficial dos normativas que complementan la ley marco de ciberseguridad. Estas obligan a las instituciones públicas y privadas -consideradas como prestadores de servicios esenciales y operadores de importancia vital- a reportar sus ciber incidentes al CSIRT Nacional (Equipo de Respuesta ante Incidentes de Seguridad Informática). Se establece que un incidente se considera “significativo” cuando interrumpe un servicio esencial, afecta la integridad física o la salud de las personas, comprometen la confidencialidad o integridad de activos informáticos, permite acceso no autorizado a redes o sistemas informáticos y/o afecta sistemas que contienen datos personales.

AUTENTICACIÓN BIOMÉTRICA: UNA SOLUCIÓN EN CHILE PARA LA PROTECCIÓN DE LOS DATOS DIGITALES

Portal Innova - El panorama del fraude digital en Chile se torna cada vez más complejo. El incremento en la digitalización de las transacciones, sumado a la creciente sofisticación de los ciberdelincuentes, exige medidas de seguridad más robustas y eficientes. En este escenario, las validaciones de identidad digital y la autenticación biométrica se posicionan como elementos fundamentales para proteger a los usuarios y sus datos, a medida que la industria avanza hacia un futuro «passwordless» (sin contraseña), dejando atrás las contraseñas tradicionales en favor de métodos más seguros y convenientes.

COLOMBIA | CIBERSEGURIDAD: INTEGRANDO BLOCKCHAIN E INTELIGENCIA ARTIFICIAL PARA FORTALECER LA PROTECCIÓN DIGITAL

dplnews - En la última década, Colombia ha experimentado una transformación digital significativa que ha impulsado el desarrollo económico y social del país. Sin embargo, este avance también ha traído consigo un aumento en las amenazas cibernéticas, lo que ha llevado a una mayor preocupación por la seguridad informática, la protección de la información y la ciberseguridad en general. En este contexto, tecnologías emergentes como el blockchain y la inteligencia artificial (IA) se perfilan como herramientas clave para reforzar la defensa contra ciberataques y garantizar la integridad de los datos en el país.

O CRESCIMENTO DO BUG BOUNTY NO BRASIL: A NOVA FRONTEIRA DA CIBERSEGURANÇA

inforchannel - A segurança digital deixou de ser um tema restrito às grandes corporações e passou a ser uma preocupação real para empresas de todos os setores. O crescimento acelerado dos ataques cibernéticos, aliado à Transformação Digital e ao avanço da regulação de proteção de Dados, tem impulsionado um novo modelo de proteção que já é amplamente adotado por grandes corporações internacionais: o Bug Bounty.

COMDCIBER DO BRASIL SE DESTACA EM EXERCÍCIO DE GUERRA CIBERNÉTICA COM 26 PAÍSES

Convergencia DIgital - O Comando de Defesa Cibernética (ComDCiber) representou o Brasil no Defence Cyber Marvel 4 (DCM4), um dos maiores exercícios de cibersegurança do mundo, coordenado pelo Exército do Reino Unido, que envolveu 26 países com participações remotas a partir de 20 localidades, tendo como sede principal Seul, na Coreia do Sul.Segundo o general Ivan de Sousa Corrêa Filho, secretário executivo do Gabinete de Segurança Institucional e futuro comandante do ComDCiber, a equipe brasileira teve desempenho de alto nível. “Ficamos muito satisfeitos”, disse a esta Convergência Digital.

OEA BUSCA MEDIR MADUREZ DE RESPUESTA A INCIDENTES CIBERNÉTICOS

dplnews - La Organización de los Estados Americanos (OEA) presentó los lineamientos “CSIRT Americas Baseline”, con el objetivo de medir la madurez de los Equipos de Respuesta ante Incidentes Cibernéticos (CSIRT, por su siglas en inglés). Dichos lineamientos, afirmó la OEA, actúan como impulsores de la Sección de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE), en el fortalecimiento de las capacidades de respuestas ante incidentes cibernéticos de la región.

¿LOS SATÉLITES SON INFRAESTRUCTURAS CRÍTICAS?

SEGURILATAM - Habitualmente, cuando se hace mención a las infraestructuras críticas que prestan servicios esenciales suele pensarse en centrales de energía, hospitales, aeropuertos... Sin embargo, las infraestructuras aeroespaciales suelen quedar relegadas a un segundo plano. Entre ellas figuran los satélites, que desempeñan un papel fundamental al prestar servicios como comunicaciones, navegación, observación terrestre o meteorología. Por ello, deben ser considerados como infraestructuras críticas que, al igual que las terrestres, requieren protección tanto física como cibernética.

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.