



INSIGHTS

APRIL 24, 2025

DIGI AMERICAS ALLIANCE MEMBERS



REPÚBLICA DOMINICANA | FIRMA ACUERDO CON COSTA RICA PARA AVANZAR EN TRANSFORMACIÓN DIGITAL SEGURA

dplnews - Durante un acto virtual en vivo, la República Dominicana y Costa Rica suscribieron un acuerdo de cooperación en materia de transformación digital y ciberseguridad, con énfasis en el reconocimiento mutuo de la firma digital, con el objetivo de promover tecnologías seguras, interoperables y centradas en el bienestar ciudadano. La iniciativa, fue rubricada por Guido Gómez Mazara, presidente del el Instituto Dominicano de las Telecomunicaciones (Indotel), y Paula Bogantes Zamora, ministra de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) de Costa Rica, quienes resaltaron la importancia de este acuerdo en el fortalecimiento de las relaciones bilaterales.

AVANZA ANÁLISIS DE INICIATIVA DE LEY DE CIBERSEGURIDAD - GUATEMALA

Congreso.gob.gt - Con el propósito de continuar con el análisis y discusión de la iniciativa 6347, ley de ciberseguridad, la Comisión de Asuntos de Seguridad Nacional, presidida por el diputado Jorge Mario Villagrán, se reunió este miércoles de forma híbrida. En esta ocasión, los diputados que integran la Sala Legislativa, definieron un paquete de 11 sanciones y penas de prisión de ciberdelitos, correspondiente al título segundo de la referida iniciativa. En la reunión los parlamentarios realizaron una inspección de las penas de prisión y las sanciones que estipulan actualmente el Código Penal, Decreto 17-73 y el Código Procesal Penal, Decreto 51-92 y de acuerdo con un cuadro comparativo definieron el aumento de penas de prisión, sanciones y multas que deberán aprobarse para prevenir y erradicar los ciberdelitos en concordancia con normativas internacionales y nacionales.

RETOS Y CLAVES ANTE NUEVAS LEYES DE CIBERSEGURIDAD Y PROTECCIÓN DE DATOS EN EL SALVADOR

E&N - Con la entrada en vigor de la Ley de Ciberseguridad y Seguridad de la Información, la Ley para la Protección de Datos Personales y las nuevas normas técnicas del Banco Central de Reserva (NRP-23 y NRP-24), las organizaciones salvadoreñas enfrentan un nuevo escenario regulatorio. Para cumplir con estas disposiciones, las empresas deben realizar ajustes profundos tanto legales como técnicos, implementar estructuras sólidas de gobernanza, y adoptar una cultura organizacional orientada a la seguridad digital.

NEARSHORING Y CIBERSEGURIDAD - MÉXICO

Aristegui - Pese al complejo escenario económico actual, el crecimiento del nearshoring está jugando un papel relevante en la evolución de la ciberseguridad industrial en México, donde las empresas globales que han invertido en el país, trajeron consigo altos estándares de seguridad, motivando a compañías locales a modernizarse. Hoy por hoy, México se ubica en el 7° lugar mundial en ciberataques y al respecto, el sector manufacturero respondió con innovación y unidad, pues las empresas han comprendido que un ataque cibernético no solo puede generar pérdidas económicas, sino también riesgos humanos en instalaciones críticas.

EL GOBIERNO IMPULSA LA FORMACIÓN EN CIBERSEGURIDAD PARA MÁS DE 6.000 AGENTES DE LA GUARDIA CIVIL - ESPAÑA

infobae - Los ministros del Interior y para la Transformación Digital y de la Función Pública, Fernando Grande-Marlaska y Óscar López, respectivamente, han firmado este lunes una declaración de intenciones para impulsar la formación en ciberseguridad de los profesionales de la Guardia Civil. Según ha detallado Interior en una nota de prensa, la iniciativa va dirigida a más de 6.000 guardias civiles que podrán beneficiarse de esta formación a distancia impartida por el Instituto Nacional de Ciberseguridad (INCIBE) en colaboración con la UNED.

POR PRIMERA VEZ FABRICARÁN CHIPS Y SUPERCOMPUTADORAS DE NVIDIA EN ESTADOS UNIDOS

dplnews - Nvidia está colaborando con sus socios de fabricación, TSMC y Foxconn, para diseñar y construir fábricas que, por primera vez, producirán supercomputadoras de Inteligencia Artificial (IA) de Nvidia de forma íntegra en Estados Unidos. Junto a TSMC, Nvidia ha puesto en funcionamiento más de un millón de pies cuadrados de espacio de fabricación para construir y probar chips Blackwell en Arizona; mientras que con Foxconn construye plantas de fabricación de supercomputadoras de IA en Texas.

SECTOR FINANCIERO REFUERZA SU DEFENSA DIGITAL: INVERSIÓN EN CIBERSEGURIDAD CRECIÓ 16%

Portafolio - El año pasado el entorno digital se caracterizó por una acelerada adopción tecnológica y una transformación digital transversal en sectores estratégicos como el financiero, manufacturero, salud, energía, transporte y administración pública. Este panorama impulsó avances significativos en materia de ciberseguridad y protección de la información en toda América Latina.

EL 80% DE ENCARGADOS DE CIBERSEGURIDAD VERÁN SUS TRABAJOS POTENCIADOS GRACIAS A LA IA GENERATIVA

Business Empresarial - Un estudio reciente de CrowdStrike indica que el 76% de los encargados de la seguridad en las organizaciones están buscando soluciones de inteligencia artificial generativa específicamente orientadas a la ciberseguridad, destacando la importancia de integrar estas herramientas para mejorar la detección de amenazas. El análisis, titulado Estado de la IA en Ciberseguridad 2024, muestra que el 80% de los responsables se decantan por la IA generativa dentro de plataformas unificadas, en lugar de herramientas aisladas. Además, una proporción similar de profesionales prefiere soluciones diseñadas específicamente para mejorar la seguridad en lugar de aplicaciones de uso general.

INVERSIONES EN CIBERSEGURIDAD, PRIORIDAD CRECIENTE PARA EMPRESAS DE AMÉRICA LATINA

America Retail - Inversiones en Ciberseguridad, prioridad creciente para empresas de América Latina, a medida que América Latina avanza hacia una era digital, la ciberseguridad se ha convertido en una de las principales preocupaciones para las empresas de la región. Con el aumento del uso de tecnologías emergentes, especialmente la inteligencia artificial (IA), tanto en el sector público como en el privado, también han crecido los riesgos asociados a los ciberataques. En este contexto, las empresas latinoamericanas están redoblando esfuerzos para proteger sus sistemas y datos frente a incidentes digitales, un desafío que ha tomado mayor relevancia debido a las nuevas legislaciones en ciberseguridad y a la creciente sofisticación de los cibercriminales.

U.S. RECIPROCAL TRADE POLICY: STRATEGIC OPPORTUNITIES FOR LATIN AMERICA AMID GLOBAL UNCERTAINTY

CSIS - The adoption of a reciprocal trade policy by the United States represents one of the most significant shifts in the country's economic approach in decades. As businesses and investors respond to this evolving landscape, both unprecedented opportunities and substantial risks emerge. The strategic recalibration of U.S. trade posture offers forward-thinking organizations a chance to address longstanding barriers while necessitating careful avoidance of potential disruptions in global supply chains and technology ecosystems.

THREE KEY WAYS TO MAKE SUPPLY CHAINS MORE RESILIENT TO CYBER RISKS

WEF - In a technologically dependent and interconnected society, managing cyber risk within global supply chains is critical. Misaligned market incentives, risk inequality and limited visibility across supply chains require new principles to boost ecosystem resilience. These three new principles should foster embeddedness, leverage advanced technology and be adaptive and proactive.

THE IMPACT OF AI REGULATIONS ON CYBERSECURITY STRATEGY

Cyber Security News - Artificial Intelligence (AI) is transforming the cybersecurity landscape, offering both powerful tools for defense and new avenues for attack. As organizations increasingly adopt AI-driven solutions to detect threats, automate responses, and analyze vast amounts of data, governments and regulatory bodies are racing to create frameworks that ensure the responsible use of these technologies.

CYBERCRIMINALS BLEND AI AND SOCIAL ENGINEERING TO BYPASS DETECTION

Help Net Security - Attackers are focusing more on stealing identities. Because of this, companies need to use zero trust principles. They should also verify user identities more carefully. Researchers analyzed thousands of alerts, mapping them to the MITRE ATT&CK framework, a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.



INSIGHTS

APRIL 24, 2025

AFRICA IN THE CROSSHAIRS AS ASIA'S CYBERCRIME RINGS GO GLOBAL

TechCentral - Asian crime syndicates behind the multibillion-dollar cyberscam industry are expanding globally including to Africa and South America, as raids in Southeast Asia fail to contain their activities, the United Nations said in a report on Monday. Criminal networks that emerged in Southeast Asia in recent years, opening sprawling compounds housing tens of thousands of workers, many trafficked and forced to scam victims around the world, have evolved into a sophisticated global industry, the United Nations Office on Drugs and Crime (UNODC) said.

CYBER-RISKS IN THE WATER SECTOR: MODERNISE AND SEGMENT TO PROTECT YOURSELF

Stormshield - A recent study by France's national Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) information systems security agency assessed the risks to which businesses and local authorities are exposed. At least 31 compromises affecting players in the water sector in France have been examined by ANSSI since 2021, warning of clear vulnerabilities in water and wastewater services. While efforts have already been made, organisations still need to strengthen their defensive stance, as befits the critical nature of their business.

THIS IS THE STATE OF PLAY IN THE GLOBAL DATA CENTRE GOLD RUSH

WEF - Data centres are proliferating rapidly, with demand driven by AI. They are not just digital infrastructure, but also high-value investment assets. Energy consumption, regulatory complexity and geopolitical tensions are potential obstacles to future growth in the sector.