DIGI AMERICAS ALLIANCE MEMBERS

MINISTERIO TIC PRESENTA AVANCES CLAVE EN LA PROTECCIÓN DIGITAL DEL ESTADO COLOMBIANO

Gov.co - Con el objetivo de avanzar hacia la consolidación de un ecosistema digital más seguro, el Ministerio de Tecnologías de la Información y las Comunicaciones, en articulación con el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) y el Centro de Investigación y Desarrollo en Tecnologías de la Información y las Comunicaciones (Cintel), realizó el encuentro "Horizonte Digital Seguro: Avances Estratégicos en Seguridad Digital para el Estado Colombiano", un espacio de alto nivel técnico que reunió a más de 130 actores clave del sector público, privado y académico.

ECUADOR AVANZA EN SU PRIMERA LEY DE INTELIGENCIA ARTIFICIAL PARA REGULAR SU USO

El Diaro - La Asamblea Nacional avanza en la formulación de su primera Ley de Inteligencia Artificial (IA), un proyecto que busca regular el uso de esta tecnología en rápida expansión, ante preocupaciones sobre privacidad y ciberseguridad. La Comisión de Educación, Cultura, Ciencia y Tecnología, Innovación y Saberes Ancestrales (CECCYT) recibió aportes de expertos el 8, 15 y 16 de julio para perfeccionar la propuesta normativa, que podría posicionar al país como referente en regulación tecnológica en la región.

TITULAR DE MITIC SE DESENTIENDE DE CRISIS EN CIBERSEGURIDAD Y PLANTEA CREAR DOS VICEMINISTERIOS - PARAGUAY

Ultima Hora - El titular del Ministerio de Tecnologías de la Información y Comunicación (MITIC), Gustavo Villate, acudió a la reunión de la mesa directiva de la Cámara Baja, liderada por el diputado Raúl Latorre, para abordar el tema de la ciberseguridad e inteligencia artificial. Rechazó responsabilidad alguna sobre los ciberataques, de los que son blancos las instituciones públicas y alegó que está realizando cambios para contrarrestar esta situación con el apoyo del Ejecutivo.

BIG DATA REVOLUCIONA LA SEGURIDAD PÚBLICA Y PRIVADA EN MÉXICO

Milenio - La era digital exige un replanteamiento en las estrategias de seguridad para la protección de información pública y privada. Es mediante la aplicación de algoritmos matemáticos, ciencia de datos e inteligencia artificial que se ofrecen las mejores soluciones en la actualidad. El uso del denominado Big Data, tecnologías y métodos para procesar y analizar grandes volúmenes de información que no pueden ser tratados con métodos tradicionales, es un modelo que permite identificar las principales zonas de riesgo, tendencias delictivas y asignación estratégica de recursos en organismos diversos.

PROPONEN CREAR UN OBSERVATORIO CONTRA CIBERODIO EN MÉXICO

Xeva - Una investigadora del Instituto Politécnico Nacional (IPN) propuso la creación del primer Observatorio Digital contra el Ciberodio en México ante el crecimiento acelerado mensajes de odio en redes sociales y plataformas digitales. Gina Gallegos García, jefa del laboratorio de ciberseguridad del Centro de Investigación en Computación (CIC), indicó la urgencia establecer un frente común que permita monitorear, analizar y combatir los discursos de odio que se generan en línea.

COMANDO DE DEFESA CIBERNÉTICA PROMOVE INTERCÂMBIO DE ESPECIALISTAS ENTRE BRASIL E EUA

Defesanet - Entre os dias 24 e 26 de junho de 2025, o Comando de Defesa Cibernética (ComDCiber) sediou, nas instalações do Centro de Instrução de Guerra Eletrônica (CIGE), o segundo Encontro de Especialistas (Subject Matter Expert Exchange – SMEE 25) com militares do Comando Conjunto Sul dos Estados Unidos da América (USSOUTHCOM). A atividade integra um Acordo de Cooperação de cinco anos, firmado entre as duas nações, com o objetivo de fortalecer os canais de comunicação e promover o intercâmbio de conhecimentos na área de Defesa Cibernética. Foram compartilhadas boas práticas relacionadas à estrutura organizacional, capacitação de pessoal e capacidades tecnológicas de ambos os países.

ADMINISTRACIÓN TRUMP DESTINARÁ CIENTOS DE MILLONES A OPERACIONES CIBERNÉTICAS OFENSIVAS Y DEFENSA EN LEY RECIENTE - EE.UU.

Infosertecla - La administración del presidente Donald Trump ha promulgado una nueva ley de impuestos y gastos, conocida extraoficialmente como la «One Big Beautiful Act», que asigna cientos de millones de dólares a la ciberseguridad, con un fuerte énfasis en el gasto militar y las capacidades ofensivas. Entre las asignaciones clave se incluyen: $250 millones para el Comando Cibernético, específicamente para iniciativas relacionadas con la inteligencia artificial, $20 millones para programas de ciberseguridad en la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA), $1 millón para operaciones cibernéticas ofensivas destinadas al Comando Indo-Pacífico de EE. UU., $90 millones para diversas necesidades del Departamento de Defensa, incluyendo apoyo de ciberseguridad para contratistas no tradicionales, y Una asignación más amplia de $2.2 mil millones para mantenimiento, que abarca el sostenimiento de «activos cibernéticos».

ESPAÑA | EL GOBIERNO DESTINA 1.157M€ A LA CIBERSEGURIDAD

dpl news - “El Gobierno de España considera fundamental la ciberseguridad, que es óptima pero siempre se puede mejorar y para ello hace un importante esfuerzo mediante un plan industrial y tecnológico para la seguridad y la defensa, con la colaboración ente el Ministerio del Interior, el de Defensa y el de para la Transformación Digital y de la Función Pública, en el que se destinan 1.157 millones para la ciberseguridad, y para el que el Instituto Nacional de Ciberseguridad ejecutará una parte importante”, aseguró hoy el secretario de Estado de Telecomunicaciones e Infraestructuras Digitales, Antonio Hernando Vera, durante la inauguración de la décima edición del Cybersecurity Summer BootCamp.

CABLES SUBMARINOS EN LA MIRA: ESTONIA PIDE NORMAS PARA RESPONDER A CORTES DELIBERADOS

dpl news - Aunque 85% de las interrupciones que sufren los cables submarinos se deben a acciones humanas no intencionadas, han aumentado los cortes provocados por actores hostiles en medio de las tensiones geopolíticas a nivel global. Durante un diálogo de alto nivel convocado por la Unión Internacional de Telecomunicaciones (UIT), la ministra de Justicia y Asuntos Digitales de Estonia, Liisa-Ly Pakosta, denunció que cables submarinos con anclaje en su país han sufrido sabotajes propiciados por una “flota fantasma rusa”, que ancla y arrastra sus buques sobre cables señalizados como protegidos.

ZERO TRUST: SEGURIDAD SIN CONFIANZA EN REDES EMPRESARIALES

ImpactoTIC - Lo dicen las cifras, el mercado de seguridad del Zero Trust está experimentando un crecimiento sustancial, con un tamaño estimado en 36.960 millones de dólares en 2024 y proyectado para alcanzar 78.700 millones de dólares en 2029 según proyecciones de la firma analista Markets and Markets, esta tecnología se ha convertido en un pilar invaluable de las estrategia de ciberseguridad moderna.

LOS CIBERDELITOS PODRÍAN COSTAR 15.6 BILLONES DE DÓLARES SI LAS PYMES NO FORTALECEN SU CIBERSEGURIDAD

infobae - Si la ciberdelincuencia fuera un país, tendría el tercer PBI más alto del mundo. Los costos globales podrían superar los 15.6 billones de dólares anuales para 2029, según Statista. Este panorama resalta la urgencia de fortalecer la seguridad digital, un desafío que afecta tanto a grandes corporaciones como a pequeñas y medianas empresas (pymes). En este contexto, según el Foro Económico Mundial y organizaciones de ciberseguridad, el 90% de las empresas reportó haber sufrido al menos un ataque cibernético en el último año, mientras que el 72 % percibe un aumento en los riesgos relacionados con la ciberseguridad.

QUANTUM COMPUTING SEEN AS TOP CYBERSECURITY THREAT BY 65% OF FIRMS

IOT World Today - Organizations worldwide are racing against time to protect their data from the looming threat of quantum computing, according to new research. Nearly two-thirds of businesses now consider quantum computing the most critical cybersecurity threat they will face in the next three to five years. The Capgemini Research Institute report, Future Encrypted: Why Post-Quantum Cryptography Tops the New Cybersecurity Agenda, found that 65% of organizations are specifically concerned about harvest-now, decrypt-later attacks, in which adversaries steal encrypted data today to decrypt it once quantum computers become powerful enough.

HOW CISOS CAN PREPARE FOR THE QUANTUM CYBERSECURITY THREAT

TechTarget - Quantum computing will mark a revolutionary change in modern computing, as well as a pivotal shift in cybersecurity. As these powerful machines make their way from theory to reality, they threaten to unravel the encryption algorithms that organizations have relied on for years to protect their data and communications systems. Industry experts and government agencies, such as NIST, the U.S. Department of Homeland Security and the U.K.'s National Cyber Security Centre, have all sounded the alarm: CISOs, the time to start preparing for quantum computing is now.

ADVANCING SYSTEMIC DEFENCE: WHAT CYBER LEADERS SAY ABOUT FIGHTING PHISHING AND FRAUD

WEF - As cybercrime rapidly evolves, phishing and scams driven by artificial intelligence are now costing the global economy over $1 trillion annually – a staggering figure that underscores the need for a more systemic and coordinated response. The World Economic Forum's Partnership against Cybercrime, in collaboration with the Institute for Security and Technology (IST), is advancing the “Systemic Defence” project, exploring how a multi-stakeholder, systemic approach can shift responsibility upstream and better defend against phishing and cyber-enabled fraud.

AI CYBERSECURITY: A PLAYBOOK FOR VALUE-DRIVEN CYBER DEFENSE

Forbes - AI is reshaping cybersecurity, bringing both promise and hype. To separate signals from noise, leaders must demand measurable value and a clear-eyed view of risk. Nearly half of large enterprises plan to use AI to detect and prevent attacks by 2025 and budgets reflect this urgency. AI-driven tools are credited with cutting breach costs by up to 31% on average.

MAJOR RAILROAD-SIGNALING VULNERABILITY COULD LEAD TO TRAIN DISRUPTIONS

Cybersecurity Dive - A newly disclosed vulnerability in train braking systems could let hackers remotely stop trains with relatively simple and inexpensive hardware, potentially causing derailments. The high-severity vulnerability, tracked as CVE-2025-1727, involves weak authentication in the protocol used to send what are known as end-of-train and head-of-train packets, radio signals that command a rail vehicle’s end-of-train device to stop the vehicle.