DIGI AMERICAS ALLIANCE MEMBERS

COLOMBIA: OCDE PRESENTA DIAGNÓSTICO SOBRE LA CONECTIVIDAD DIGITAL Y LOS MERCADOS DE COMUNICACIONES

trendTIC - La Organización para la Cooperación y el Desarrollo Económicos (OCDE) presentó ayer el informe “Revisión de la conectividad digital en Colombia”, un diagnóstico que analiza la transformación de los mercados de comunicaciones en el país y plantea orientaciones para fortalecer la competencia, la inversión y la inclusión digital. La presentación se realizó en el marco del Colombia Digital Summit 2026, encuentro regional que reúne en Cartagena a autoridades, reguladores, expertos internacionales y líderes del sector tecnológico para debatir sobre conectividad, regulación, inteligencia artificial y economía digital.

MUNDIAL 2026 DISPARA ALERTAS POR ESTAFAS DIGITALES EN MÉXICO

Addictware - El Mundial 2026 con sedes en México, EE.UU. y Canadá, es considerado por expertos en ciberseguridad como un evento de alto riesgo digital por la enorme actividad económica y digital que genera con la compra de boletos, contratación de plataformas de streaming, viajes y hospedaje y una temporada alta para el comercio electrónico. Analizamos las estafas más comunes que se aprovechan de este tipo de eventos masivos donde la combinación de emoción, urgencia y disposición a comprar crea el entorno perfecto para fraudes digitales.

CONFERÊNCIA DESTACA PAPEL DO JUDICIÁRIO NA PROTEÇÃO DE CRIANÇAS E ADOLESCENTES NO AMBIENTE DIGITAL - BRASIL

STJ - A VII Conferência Ibero-Americana dos Direitos da Criança foi encerrada nesta quarta-feira (25), no auditório externo do Superior Tribunal de Justiça (STJ). Durante dois dias, o evento reuniu especialistas nacionais e estrangeiros em um grande debate sobre os desafios da proteção de crianças e adolescentes no ambiente digital, com destaque para a Lei 15.211/2025 (Estatuto Digital da Criança e do Adolescente – ECA Digital), que recentemente entrou em vigor no Brasil.

ENTIDADES PEDEM APROVAÇÃO URGENTE DO REDATA E DE CONVÊNIO PARA DATA CENTERS - BRASIL

teletime - Diversas entidades que atuam no setor de Tecnologia da Informação e Comunicação (TIC) – incluindo Telcomp, Associação Neo e Brasscom – divulgaram nesta terça-feira, 24, um manifesto pedindo a aprovação urgente do Regime Especial de Tributação para Serviços de Data Center (Redata) e de um convênio no âmbito do Conselho Nacional de Política Fazendária (Confaz) para redução do ICMS sobre equipamentos de data center. O capex de um data center de grande porte (100 MW) no Brasil é, em média, 34% superior ao de uma estrutura similar nos Estados Unidos. A diferença, segundo as entidades, é a carga tributária sobre bens de capital e tecnologia, sendo que o ICMS representa cerca de 64% dessa tributação.

CISCO REDEFINE A SEGURANÇA PARA A FORÇA DE TRABALHO AGÊNTICA

dpl News - A Cisco anunciou hoje inovações de segurança projetadas para o ecossistema de IA agente, onde o software não apenas responde a perguntas, mas também executa ações. Na RSA Conference 2026, a Cisco apresenta soluções para abordar questões de segurança de IA e remover uma das principais barreiras à adoção de agentes. Ao estabelecer identidades confiáveis, aplicar controles rigorosos de Acesso Zero Trust, fortalecer agentes antes da implantação, aplicar barreiras em tempo de execução e fornecer às equipes do Centro de Operações de Segurança (SOC) as ferramentas para interromper ameaças na velocidade da máquina, a Cisco está construindo a segurança na base da economia emergente de IA.

CHECK POINT SOFTWARE LANZA ARQUITECTURA DE SEGURIDAD INTEGRAL PARA PROTEGER LA NUEVA INFRAESTRUCTURA DE IA DE CHILE, EN PLENA EXPLOSIÓN DE INVERSIÓN EN DATA CENTERS

Seguridad & Defensa - Check Point® Software Technologies Ltd., pionero y líder global en soluciones de ciberseguridad, ha lanzado su AI Factory Security Architecture Blueprint: una arquitectura de referencia integral, probada por proveedores, diseñada para proteger la infraestructura de IA privada desde la capa de hardware hasta la de aplicación. El anuncio llega en un momento crítico para Chile, que se consolida como el segundo mercado de data centers más grande de América Latina y enfrenta una superficie de ataque radicalmente nueva que las soluciones convencionales no cubren.

CÓMO LA GEOPOLÍTICA ESTÁ INFLUYENDO EN LA CIBERSEGURIDAD

El Mostrador - En 2026, la geopolítica continuará siendo el principal factor que influye en las estrategias generales de mitigación del riesgo cibernético. La última versión del estudio del World Economic Forum (WEF) y Accenture, mostró que 64% de las organizaciones a nivel mundial está considerando ciberataques con motivación geopolítica, como lo son la interrupción a la infraestructura crítica o el espionaje. Y, de hecho, el 91% de las organizaciones más grandes ha modificado sus estrategias de ciberseguridad debido a la volatilidad geopolítica.

FCC BANS NEW FOREIGN-MADE ROUTERS OVER SUPPLY CHAIN AND CYBER RISK CONCERNS - USA

The Hacker News - The U.S. Federal Communications Commission (FCC) said on Monday that it was banning the import of new, foreign-made consumer routers, citing "unacceptable" risks to cyber and national security. The action was designed to safeguard Americans and the underlying communications networks the country relies on, FCC Chairman Brendan Carr said in a post on X. The development means that new models of foreign-produced routers will no longer be eligible for marketing or sale in the U.S. The move comes in the wake of a national security determination provided by Executive Branch Agencies, Carr added.

NIST EXPANDS CSF 2.0 TOOLKIT WITH QUICK-START GUIDES ALIGNING CYBER RISK, RISK MANAGEMENT, WORKFORCE STRATEGY - USA

Industrial Cyber - The U.S. NIST (National Institute of Standards and Technology) released two new NIST Cybersecurity Framework (CSF) 2.0 quick-start guides (QSG), adding to an expanding portfolio of implementation resources that offer tailored pathways for different audiences to engage with CSF 2.0. One document positions cybersecurity risk as a core component of enterprise risk management and integrates it with workforce planning to improve how organizations assess, communicate, and respond to threats, while the other explains what informative references are and how they support achieving the outcomes of CSF 2.0. NIST published the final version of NIST Special Publication (SP) 1308, NIST Cybersecurity Framework 2.0: Cybersecurity, Enterprise Risk Management, and Workforce Management Quick-Start Guide, which draws on concepts and practices from enterprise risk management, cybersecurity risk management, and workforce management to help organizations improve communication about cybersecurity risks, plan workforce decisions, and implement risk-informed responses.

TRUMP ADMINISTRATION'S EO ON CYBERCRIME AND A CYBER STRATEGY FOR AMERICA - USA

The National Law Review - On Friday, March 6, 2026, the White House issued a sweeping Executive Order (EO) titled, "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens." The EO reflects what most organizations already know all too well: cybercrime is no longer an episodic threat. It is a relentless, organized enterprise that is inflicting devastating financial, operational, and human harm across the globe and, in particular, in the United States. The Trump Administration also published in March a Cyber Strategy for America, laying out six pillars underpinning the cyber strategy: Shape Adversary Behavior, Promote Common Sense Regulation, Modernize and Security Federal Government Networks, Secure Critical Infrastructure, Sustain Superiority in Critical Technologies, and Build Talent and Capacity.

CYBERCRIME DISRUPTION DEMANDS GLOBAL TRUST AND COORDINATION - UK

Gov Info Security - Dismantling cybercrime groups requires more than technical capability. It demands trust, coordinated strategy and cross-border collaboration, said Paul Foster, head of the National Cyber Crime Unit at the U.K.'s National Crime Agency, or NCA. Cross-border law enforcement collaboration has matured significantly since the pandemic. A renewed push beginning early 2023 - among Five Eyes agencies, European partners and Europol - produced a shared incident response framework built around four principles: collect, store, analyze and engage. But underpinning every operation is something more fundamental, he said.