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

REPÚBLICA DOMINICANA AFIANZA SU LIDERAZGO REGIONAL EN TRANSFORMACIÓN DIGITAL CON INVERSIÓN PÚBLICA Y COLABORACIÓN INTERNACIONAL

Infobae - Los retos de la transformación digital en América Latina exigen construir infraestructura de última generación y asegurar que su impacto llegue a todos los segmentos de la población, especialmente en zonas rurales y ciudades marginadas. El caso de la República Dominicana ilustra cómo pueden implementarse estrategias integrales que logran avances medibles en conectividad, inclusión y desarrollo de habilidades digitales.

ANPD GANHA AUTONOMIA E REFORÇA CONTROLE SOBRE USO DE DADOS NA INTERNET - BRASIL

Fast Company Brasil - O Senado aprovou na última terça-feira (24), em Brasília, a medida provisória que transforma a Autoridade Nacional de Proteção de Dados em Agência Nacional de Proteção de Dados (ANPD). A proposta foi votada às vésperas do fim do prazo de vigência e recebeu aval na forma de projeto de lei de conversão. A mudança ocorre para fortalecer a estrutura do órgão responsável por fiscalizar o uso de dados no país.Segundo o Senado, essa mudança permite a regulamentação do Estatuto Digital da Criança e do Adolescente (ECA), que começa a valer em março. A matéria segue agora para sanção presidencial.

PROJETO PROPÕE INCENTIVO FISCAL PARA FORTALECER FISCALIZAÇÃO NA CIBERSEGURANÇA - BRASIL

Capital Digital - Tramita no Senado Federal o Projeto de Lei Complementar (PLP) 246/2025, de autoria do senador Mecias de Jesus, que propõe mudanças nas condições para que empresas estrangeiras de segurança cibernética tenham acesso à redução das alíquotas do Imposto sobre Bens e Serviços (IBS) e da Contribuição sobre Bens e Serviços (CBS). Atualmente, a Lei Complementar 214 estabelece redução de 60% nas alíquotas do IBS e da CBS para empresas de cibersegurança, desde que contem com sócio brasileiro detentor de, no mínimo, 20% de participação societária.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 26, 2026

BRASIL E COREIA DO SUL REFORÇAM COOPERAÇÃO BILATERAL EM MINERAIS CRÍTICOS

Business Moment - A visita de Estado do presidente Luiz Inácio Lula da Silva a Seul, nesta segunda-feira (23), marcou um novo capítulo nas relações diplomáticas entre Brasil e Coreia do Sul. Em reunião de cúpula com o presidente sul-coreano, Lee Jae-myung, os mandatários selaram o compromisso de elevar a relação bilateral ao patamar de parceria estratégica. O encontro, que ocorre 21 anos após a última visita oficial de um presidente brasileiro ao país, resultou na assinatura de dez memorandos de entendimento (MoUs) que abrangem desde a exploração de minerais críticos até a cooperação em inteligência artificial e segurança cibernética.

SEGUNDO PROTOCOLO DE BUDAPEST: COLOMBIA PREPARA REGLAS PARA PRUEBAS DIGITALES TRANSFRONTERIZAS

ImpactoTIC Colombia - El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Equipo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert) y la Cancillería lideraron un taller técnico orientado a la sensibilización de proveedores de servicios digitales sobre el Segundo Protocolo Adicional del Convenio de Budapest. El encuentro, que contó con el respaldo del proyecto GLACY-e de la Unión Europea (Global Action on Cybercrime Enhanced) y el Consejo de Europa, busca preparar al país para una eventual ratificación de este instrumento jurídico, diseñado para agilizar la obtención transfronteriza de pruebas electrónicas en investigaciones criminales.

COLOMBIA Y MÉXICO CONSOLIDAN ALIANZA PARA FORTALECER LA COOPERACIÓN REGULATORIA EN COMUNICACIONES

trendTIC - La Comisión de Regulación de Comunicaciones (CRC) y la Comisión Reguladora de Telecomunicaciones (CRT) fortalecen la cooperación técnica y regulatoria en un marco de colaboración que busca promover el intercambio de experiencias y contribuir al análisis conjunto de los desafíos del ecosistema digital, favoreciendo el desarrollo de mercados más eficientes, competitivos e innovadores. El Memorando establece un marco no vinculante de colaboración, dentro de las competencias de cada entidad, enfocado en el intercambio de conocimiento técnico y buenas prácticas regulatorias. Su objetivo es contribuir al análisis y abordaje de los retos actuales y futuros del sector de las telecomunicaciones, la radiodifusión y los servicios digitales, en un contexto de acelerada transformación tecnológica.

COMANDANTES DEL CONTINENTE DEBATEN SOBRE CRIMEN ORGANIZADO Y CIBERSEGURIDAD

Ultima Hora - El martes se dio apertura al encuentro, con presencia de Santiago Peña, presidente de la República, a la Conferencia de Ejércitos Americanos que se desarrolla en Asunción hasta este viernes 27 para analizar los “desafíos multidimensionales para la defensa y la seguridad estratégica de los países integrantes”. El comandante del Ejército Paraguayo y presidente de la Conferencia de Ejércitos Americanos, general Manuel Rodríguez Sosa, fue el encargado de las palabras de apertura de la sesión inaugural de la Conferencia.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 26, 2026

EL MAYOR RETO DIGITAL DEL MUNDIAL 2026: ATAQUES CIBERNÉTICOS, APUESTAS Y TRÁFICO SIN PRECEDENTES

pulzo - Con la proximidad del Mundial de la FIFA en junio de 2026, no solo los estadios y equipos estarán bajo presión; el entorno digital global también enfrentará uno de sus mayores desafíos. Este evento deportivo, catalogado como el más observado del planeta, desencadena una enorme concentración de actividades en línea en sectores tan diversos como apuestas digitales, gaming, ventas de boletos, comercio electrónico, medios de comunicación y redes sociales. La simultaneidad de millones de usuarios interactuando—ya sea buscando información, compartiendo emociones o realizando apuestas—genera un escenario inédito de alta demanda en infraestructura tecnológica.

LA INTELIGENCIA ARTIFICIAL PERMITE EJECUTAR CIBERATAQUES EN SOLO 27 SEGUNDOS

Infobae - La aceleración en *el uso de inteligencia artificial (IA) por parte de grupos de ciberdelincuentes* ha provocado que un ataque sofisticado pueda iniciarse en apenas 27 segundos, un fenómeno que está transformando radicalmente la seguridad digital a escala global. De acuerdo con el Informe Global de Amenazas 2026 publicado por la compañía CrowdStrike, la combinación de innovaciones en IA y la adaptación instantánea de los atacantes está recortando drásticamente los tiempos de respuesta y aumentando el volumen de amenazas contra infraestructuras corporativas, haciendo que los responsables de seguridad enfrenten un escenario sin precedentes

CHINA-LINKED HACKERS BREACHED DOZENS OF TELECOMS, GOVERNMENT AGENCIES

Cybersecurity Dive - Hackers working for the Chinese government broke into more than 50 telecommunications companies and government agencies in 42 countries, in a campaign that exploited cloud platforms' legitimate features to hide the attackers' tracks. "The attacker was using API calls to communicate with [software-as-a-service] apps as command-and-control (C2) infrastructure to disguise their malicious traffic as benign," researchers at Google's Threat Intelligence Group and Mandiant said in a report on Wednesday. Google said the "prolific, elusive" China-linked hacker team, which it tracks as UNC2814, "has a long history of targeting international governments and global telecommunications organizations across Africa, Asia, and the Americas."

GENAI MISUSE & RANSOMWARE DRIVE SURGE IN CYBER ATTACKS

ITBrief - Organisations worldwide faced an average of 2,090 cyber attacks per week in January 2026, as ransomware activity increased and broader use of generative AI tools raised the risk of data exposure, according to new research from Check Point Research. The figure was up 3% from December and 17% year on year. Check Point attributed the rise to more frequent ransomware campaigns and gaps in governance around GenAI use on corporate networks. "January's data shows that cyber attacks are not only increasing but becoming more refined and opportunistic," said Omer Dembinsky, data research manager at Check Point Research. "Ransomware operators are accelerating their campaigns while unchecked GenAI usage is opening new blind spots for organizations. Prevention-first, real-time protection powered by AI is the only effective way to stop attacks before they cause operational or financial damage."