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 TREND MICRO

COLOMBIA PREPARA ASIGNACIÓN DE ESPECTRO PARA MEJORAR CONECTIVIDAD RURAL

bnamericas - Colombia prepara un proceso para asignar espectro radioeléctrico a actores locales, con el objetivo de ampliar la conectividad de internet fijo residencial en zonas rurales y apartadas del país. La iniciativa contempla la entrega de permisos de uso local de la banda de 900MHz, considerada óptima para entornos rurales por sus características de propagación, con la meta de expandir el acceso a internet en estas áreas. El ministerio TIC evalúa entregar espectro a comunidades de conectividad y a proveedores de redes y servicios de telecomunicaciones que al 30 de junio de 2025 contaran con menos de 30.000 accesos.

CHILE SE INTEGRA AL CENTRO DE CIBERCAPACIDADES DE LATINOAMÉRICA Y EL CARIBE

Segurilatam - La Agencia Nacional de Ciberseguridad de Chile (ANCI) ha anunciado su incorporación oficial como nuevo miembro del Centro de Cibercapacidades de Latinoamérica y el Caribe (LAC4, por sus siglas en inglés de Latin America and Caribbean Cyber Competence Centre). Este centro internacional promueve la cooperación y el aprendizaje conjunto en ciberseguridad entre América Latina, el Caribe y Europa. La directora de LAC4, Liina Areng, ha destacado que la incorporación de Chile representa un paso relevante para fortalecer la seguridad digital en Sudamérica y refleja el compromiso permanente de la Unión Europea con el desarrollo de un entorno digital más seguro en la región.

SETOR DA SAÚDE É ALVO FÁCIL PARA HACKERS NO BRASIL, ALERTAM ESPECIALISTAS

Viva - Nesta quarta-feira, 28 de janeiro, o Brasil celebra o Dia Internacional da Proteção de Dados em um cenário de vulnerabilidade digital crescente. Instituída em 2006, a data marca o aniversário da Convenção 108 do Conselho da Europa — o primeiro tratado internacional para garantir a privacidade, assinado em 1981. Contudo, décadas após o compromisso global, a segurança cibernética nacional enfrenta desafios. Dados do Relatório de Estatísticas Globais de Ataques Cibernéticos da Check Point mostram um aumento de 38% nas investidas criminosas online apenas em dezembro, ritmo que supera a capacidade de defesa de boa parte das organizações.

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 30, 2026

ACORDO ENTRE BRASIL E UNIÃO EUROPEIA SOBRE DADOS PESSOAIS IMPULSIONA COOPERAÇÃO CIENTÍFICA E DIGITAL

Radar Digital Brasil - O Governo do Brasil e a União Europeia anunciaram o reconhecimento recíproco da equivalência dos padrões elevados e confiáveis adotados por seus sistemas de proteção de dados de pessoas e da privacidade. A decisão estabelece um marco jurídico de confiança para a transferência internacional de dados de pessoas entre Brasil e União Europeia, assegurando proteção de direitos e segurança jurídica sempre que a circulação de dados for necessária para atividades econômicas, prestação de serviços, oportunidades para cooperação em ciência, tecnologia, pesquisa científica e uso de plataformas digitais com operações internacionais.

EN 2026 SE MULTIPLICARÁN LOS RIESGOS EN CIBERSEGURIDAD; LOS CIBERDELINCUENTES SE ENFOCAN EN MÉXICO COMO OBJETIVO PRIORITARIO

Diario Noticias Web - El presidente del Consejo de Administración de Proyectos y Suministros Interdisciplinarios (PSI-México) e investigador del Instituto Politécnico Nacional, Ezequiel Aguiñiga Tinoco, señaló que el 2025 se caracterizó por la adopción acelerada de la inteligencia artificial en el mundo, que está transformando la productividad; y para este 2026, se multiplicará de manera significativa el panorama de riesgos en materia de ciberseguridad, especialmente en nuestro país.

CIBERSEGURIDAD EN AMÉRICA LATINA 2025: BRECHAS CRÍTICAS E IMPACTO DE LA IA

ImpactoTIC - América Latina y el Caribe muestran avances modestos en ciberseguridad, pero persisten vacíos institucionales que ponen en riesgo servicios públicos y economías digitales. Según el ‘Informe de Ciberseguridad 2025’ del BID y la OEA, solo 13 países tienen la capacidad de implementar sus estrategias nacionales, enfrentando nuevos desafíos por el uso malicioso de la IA.

DÍA INTERNACIONAL DE LA PROTECCIÓN DE DATOS PERSONALES: POR QUÉ ES CLAVE EN LA ERA DIGITAL

La 100 - El 28 de enero se conmemora el Día Internacional de la Protección de Datos Personales, fecha vinculada a la apertura a la firma del Convenio 108 del Consejo de Europa. Ese instrumento fue el primer pacto global sobre privacidad y marcó el comienzo de normas internacionales sobre la protección de datos personales. El Instituto Interamericano de Derechos Humanos (IIDH) es Miembro Observador del Comité Consultivo del Convenio 108 desde 2021 y dicta desde ese mismo año el Diplomado Internacional “El Derecho Humano a la Privacidad y a la Protección de los Datos Personales”. La tercera edición estaba prevista para la segunda mitad de 2023.

CYBER CENTRE RELEASES RANSOMWARE THREAT OUTLOOK 2025 TO 2027 - CANADA

Government of Canada - Today, the Canadian Centre for Cyber Security (Cyber Centre), part of the Communications Security Establishment Canada (CSE), released its Ransomware Threat Outlook 2025 to 2027, its latest assessment of ransomware threats facing Canada. The modern ransomware landscape is a highly sophisticated and interconnected ecosystem that is constantly evolving. Understanding current and emerging trends is critical to helping Canadians better prepare for and mitigate ransomware risks.

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 30, 2026

LATIN AMERICA CYBER SECURITY MARKET ANALYSIS: GROWTH, TRENDS, AND FORECAST (2026-2034)

Vocal Media - The digital landscape in Latin America is evolving at breakneck speed, but this rapid technological expansion has a dark side. Recent studies indicate that organizations in the region now face an average of 2,716 cyber attacks per week, a figure that stands 39% higher than the global average. As businesses scramble to protect their digital assets, the Latin America cybersecurity market has become a critical focal point for investors, governments, and enterprise leaders alike.

HEALTHCARE CYBERSECURITY MARKET TO REACH US$ 78.78 BILLION BY 2033 AT 16.5% CAGR; NORTH AMERICA LEADS WITH 41% SHARE | KEY PLAYERS PALO ALTO NETWORKS, CROWDSTRIKE, CHECK POINT

openPR - The healthcare cybersecurity market reached US$ 20.01 billion in 2024 and is expected to reach US$ 78.78 billion by 2033, growing at a CAGR of 16.5% during the forecast period 2025-2033. Market growth is driven by the rapid digitalization of healthcare systems, increasing adoption of electronic health records and connected medical devices, and the rising frequency of cyberattacks targeting healthcare data. Healthcare organizations are investing heavily in advanced cybersecurity solutions to protect sensitive patient information, ensure regulatory compliance, and maintain operational continuity. The market is high in North America, supported by stringent data protection regulations and advanced healthcare IT infrastructure, while Europe follows with strong compliance-driven adoption. Asia-Pacific is emerging as a high-growth region due to expanding healthcare digitization, growing awareness of data security risks, and increasing investments in cybersecurity frameworks across hospitals and healthcare networks.

APTS, CYBERCRIMINALS WIDELY EXPLOITING WINRAR VULNERABILITY

Security Week - Tracked as CVE-2025-8088, the high-severity bug was patched on July 30, after being exploited in the wild as a zero-day by the Russia-linked hacking group named RomCom (also known as Storm-0978, Tropical Scorpius, and UNC2596). The issue is described as a path traversal flaw in WinRAR for Windows that can be abused for arbitrary code execution using crafted archive files. According to GTIG, APTs and cybercrime groups have exploited the security defect via malicious files hidden within the Alternate Data Streams (ADS) of a decoy file inside an archive.

AI-POWERED POLYMORPHIC ATTACK LURES VICTIMS TO PHISHING WEBPAGES

CSO - AI-fueled attacks can transform an innocuous webpage into a customed phishing page. The attacks, revealed in a research from Palo Alto Networks' Unit 42, are clever in how they combine various obfuscation techniques. The combination though can be lethal, difficult to discover, and represent yet another new offensive front in the use of AI by bad actors to compromise enterprise networks. The attack starts with an original and ordinary webpage then attackers add client-side API calls to LLMs that can dynamically generate malicious JavaScript code in real time. This polymorphic technique is dangerous for several reasons.