DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 2, 2026

DIGI AMERICAS ALLIANCE MEMBERS

ASAMBLEA NACIONAL APRUEBA LEY ORGÁNICA PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD - ECUADOR

Ecuador Comunicacion - Con 83 votos afirmativos, el Pleno de la Asamblea Nacional resolvió la objeción parcial al Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, sobre la base del informe no vinculante de la Comisión de Soberanía, Integración y Seguridad Integral. La ley establece una arquitectura moderna y constitucionalmente compatible para robustecer la ciberseguridad nacional, proteger infraestructura crítica y garantizar la continuidad de servicios esenciales. Además, articula un modelo coherente de gobernanza digital.

COLOMBIA 5.0: LA APUESTA POR UNA TRANSFORMACIÓN DIGITAL CON ROSTRO TERRITORIAL

el campesino.co - Colombia inicia una nueva etapa en su camino hacia la transformación digital. Con el lanzamiento de Colombia 5.0, el Ministerio de Tecnologías de la Información y las Comunicaciones presenta una visión que pone la tecnología al servicio del desarrollo territorial, la equidad y la competitividad, superando el enfoque centrado únicamente en la adopción tecnológica. La iniciativa marca la evolución de Colombia 4.0 hacia un modelo alineado con el concepto de Sociedad 5.0, en el que la innovación se articula directamente con las necesidades de las personas, las comunidades y los sectores productivos.

CIBERATAQUES Y FALLAS TÉCNICAS ELEVAN EL RIESGO DE PÉRDIDA DE DATOS: EXPERTOS LLAMAN A REFORZAR PRÁCTICAS DE RESPALDO - CHILE

trendTIC - La digitalización en la vida personal y laboral ha elevado la exposición a riesgos asociados a la pérdida de información. En Chile, los delitos informáticos han mostrado una tendencia al alza en los últimos años, impulsados por el avance del comercio electrónico y el uso intensivo de dispositivos personales para almacenar datos críticos. De acuerdo con la Policía de Investigaciones de Chile (PDI), a través de su Brigada Investigadora del Cibercrimen, los delitos asociados a fraudes digitales, suplantación de identidad y accesos indebidos a sistemas han aumentado en los últimos años, especialmente aquellos vinculados a ingeniería social, evidenciando un escenario de mayor vulnerabilidad para usuarios y organizaciones.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 2, 2026

BRASIL AVANÇA EM DEFESA CIBERNÉTICA E GESTÃO DE RISCO HUMANO GANHA PROTAGONISMO ESTRATÉGICO NO NOVO MAPEAMENTO DO SETOR - BRASIL

Revista Seguranca - O lançamento do mapeamento conduzido por profissionais do mercado em parceria com o MITI (Markets, Innovation & Technology Institute) — responsável pelo Mapa do Ecossistema Brasileiro de Defesa Cibernética — marca um novo momento para o setor de tecnologia e segurança no Brasil. A iniciativa organiza, estrutura e dá visibilidade a um ecossistema que vinha crescendo de forma acelerada, mas ainda carecia de uma visão consolidada sobre seus players, competências e lacunas estratégicas.

ECONOMIA – BANCO CENTRAL ESTUDA REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL E CRIPTOGRAFIA QUÂNTICA PARA AUMENTAR SEGURANÇA NO SETOR FINANCEIRO E COMBATER FRAUDES - BRASIL

Reporter Maceio - O Banco Central (BC) brasileiro está se aprofundando em estudos relacionados à regulamentação de tecnologias emergentes, como a Inteligência Artificial (IA) e a computação quântica, com ênfase na segurança cibernética. Essa iniciativa foi destacada por Carlos André de Melo Alves, coordenador do Departamento de Regulação do Sistema Financeiro do BC. Carlos André afirmou que a autarquia está em um processo de aprendizado e diálogo com outros reguladores, especialmente no que diz respeito à criptografia quântica.

COMITÊ GESTOR DA INTERNET ATUALIZA CARTILHA CONTRA GOLPES ONLINE - BRASIL

Diario do RN - O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), grupo dedicado a pensar a segurança dentro do Comitê Gestor da Internet no Brasil (CGI.Br) lançou uma versão atualizada de sua cartilha sobre segurança, com dois volumes dedicados à educação contra golpes e contra fraudes online. Eles destacam, em linguagem fácil e acessível, a dinâmica dos golpes mais relevantes aplicados atualmente, detalhados e baseados em pesquisa prévia, métricas que remetem à publicidade para a internet e ao uso de dados vazados.

UE Y AMÉRICA LATINA Y EL CARIBE REFUERZAN SU COLABORACIÓN EN CIBERSEGURIDAD Y CONECTIVIDAD SEGURA

EEAS - Durante tres días de intensas sesiones, los socios de la Unión Europea y América Latina y el Caribe abordaron los temas prioritarios de su agenda digital compartida, destacando: Resiliencia cibernética y respuesta ante incidentes: A través del programa EU-LAC Cyber-SHIELD, se avanzó en la cooperación para fortalecer la seguridad de sistemas críticos y la capacidad de reacción ante ciberamenazas. Alianzas público-privadas en ciberseguridad: Se organizaron sesiones de matchmaking para fomentar colaboraciones entre el sector público y privado, fortaleciendo la conectividad segura en la región. Conectividad segura y tecnologías avanzadas: Se impulsaron iniciativas conjuntas en 5G seguro y conectividad satelital confiable, buscando garantizar redes digitales resilientes y confiables.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 2, 2026

CISA URGES ENDPOINT MANAGEMENT SYSTEM HARDENING AFTER CYBERATTACK AGAINST US ORGANIZATION - USA

CISA - CISA is aware of malicious cyber activity targeting endpoint management systems of U.S. organizations based on the March 11, 2026 cyberattack against U.S.-based medical technology firm Stryker Corporation, which affected their Microsoft environment.[1] To defend against similar malicious cyber activity, CISA urges organizations to harden endpoint management system configurations using the recommendations and resources provided in this alert. CISA is conducting enhanced coordination with federal partners, including the Federal Bureau of Investigation (FBI), to identify additional threats and determine mitigation actions.

PALO ALTO NETWORKS ANUNCIA INNOVACIONES PARA FORTALECER LA CIBERSEGURIDAD EN LA ERA DE LA IA AVANZADA

Revista Summa - En un momento en que la adopción de inteligencia artificial, el uso de agentes autónomos y la dependencia del navegador como plataforma de trabajo están transformando los entornos digitales, se presentaron cuatro innovaciones que responden a nuevas y crecientes necesidades de seguridad. Las soluciones más recientes ofrecen caminos para reforzar la resiliencia operativa, proteger identidades humanas y no humanas, prevenir interrupciones críticas y habilitar modelos de trabajo basados en IA de manera segura. Para organizaciones de América Latina, donde la digitalización acelerada continúa ampliándose, estas capacidades representan una oportunidad para fortalecer la infraestructura y preparar al negocio para escenarios cada vez más complejos.

ONLY 5% OF ORGANIZATIONS FULLY TRUST CYBERSECURITY VENDORS, REVEALS SOPHOS

tiinside - In Sophos' independent global study on the relationship between companies and cybersecurity solution providers, 95% of respondents stated they do not have full confidence in their suppliers. Based on responses from 5.000 organizations in 17 countries, including Brazil, the study examines one of the most urgent and neglected needs in cybersecurity: trust. The report Cybersecurity Trust Reality 2026 This is one of the most comprehensive studies ever conducted on trust in cybersecurity and its impact on operational risk and executive board decision-making. The survey reveals a critical challenge faced by CISOs: trust in cybersecurity vendors is fragile, difficult to measure, and increasingly decisive in shaping organizations' risk posture, both at the operational and strategic levels.

AI WILL DRIVE SCALABLE CYBERATTACKS IN 2026: GOOGLE CLOUD

Mexico Business Review - By 2026, AI will transition from an exceptional tool to the operational norm for cyber adversaries, enabling automated attacks at a massive scale, says Google Cloud Security. This transformation, alongside the exploitation of hypervisors and critical supply chains, redefines security priorities for enterprises in Mexico and the Latin American region. "Organizations must be prepared for the threats and the adversaries that leverage AI," says Jon Ramsey, Vice President and General Manager, Google Cloud Security. This warning is relevant for the Latin American market, where the rapid adoption of AI agents without robust controls creates significant risks for compliance and the protection of intellectual property.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 2, 2026

WHY THE AI ECONOMY CAN'T RELY ON A SINGLE DIGITAL SUEZ

WEF - When several undersea cables were severed in the Red Sea in early 2024 – initially attributed to accidental damage but later suspected to be connected to Houthi attacks on shipping off Yemen – the impact was felt almost instantly. Latency between Europe, Asia and Africa spiked overnight. Cloud services slowed. Financial transactions faltered. Hundreds of companies and millions of users experienced disruptions without ever knowing why. For data centres and markets, the impact was immediate. For governments, it should have been a wake-up call. This incident was only one of the suspected sabotage attacks on undersea cables, with at least 11 in the Baltic Sea between 2023 and 2024 and multiple incidents in the waters around Taiwan in 2025. Not to mention the dozens of accidents occurring from fishing and unintentional anchor damage to the nearly 600 worldwide undersea cables.

DEMOCRATIZING CYBERCRIME: HOW SOPHISTICATED AI SYSTEMS ARE EMPOWERING A NEW GENERATION OF CYBERCRIMINALS

Global Initiative - AI is once again in the news for the wrong reasons, with recent developments at two major companies – Anthropic and OpenAI – introducing an unprecedented cybersecurity vulnerability into global digital infrastructure. On 26 March, Anthropic accidentally leaked internal documents detailing a new tool named 'Claude Mythos', described by the company as 'by far the most powerful AI model we've ever developed'. The unreleased materials, made publicly accessible in error, also revealed that Anthropic is seriously concerned about the system's 'near-term risks in the realm of cybersecurity'. In response to the incident, a company spokesperson said Anthropic was proceeding with 'extra caution' ahead of the release of Mythos. Nevertheless, the news sent alarm bells ringing across the cybersecurity industry, as concerns were raised that the development of offensive AI capabilities – used to plan or execute malicious activity – is outpacing the development of defensive technology.