DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2025

DIGI AMERICAS ALLIANCE MEMBERS

LANÇADA ALIANÇA NACIONAL PARA PREVENIR GOLPES NA INTERNET - BRASIL

RadioAgência - O Ministério da Justiça e Segurança Pública e a Federação Brasileira de Bancos lançaram uma aliança nacional para combater fraudes bancárias digitais. O objetivo é criar medidas para prevenir golpes na internet e melhorar o atendimento às vítimas. O governo vai trabalhar com bancos, empresas de telefonia, comércio online e redes sociais para desenvolver ações de segurança. A cada dois meses, um comitê gestor avaliará o avanço das propostas.

VENDA DE DADOS DE ÍRIS PARA IA: RISCOS PARA SEGURANÇA DIGITAL - BRASIL

FolhaDeCianorte - A comercialização de dados biométricos, como a íris, para empresas de Inteligência Artificial (IA) tem gerado preocupação com a segurança digital e a privacidade. No Brasil, cerca de 500 mil pessoas tiveram sua íris escaneada em troca de criptomoedas por meio do projeto Worldcoin, suspenso pelo governo devido a questões regulatórias. A coleta e o armazenamento desses dados representam um risco elevado, pois, ao contrário de senhas, a íris é imutável e, se comprometida, pode ser explorada por cibercriminosos.

GOVERNO DE SERGIPE FORTALECE SEGURANÇA CIBERNÉTICA EM PARCERIA COM O GOVERNO FEDERAL - BRASIL

f5news - No último final de semana, representantes da Empresa Sergipana de Tecnologia da Informação (Emgetis) estiveram em Brasília (DF) para uma reunião estratégica com o Gabinete de Segurança Institucional da Presidência da República (GSI/PR). O encontro, realizado no Palácio do Planalto, marcou a premente adesão do Governo de Sergipe à Rede Federal de Gestão de Incidentes Cibernéticos, fortalecendo a capacidade do estado na resposta e prevenção a ameaças digitais.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2025

REALIZAN CONVERSATORIO SOBRE EL PAPEL DE LA INTELIGENCIA ARTIFICIAL EN SEGURIDAD PÚBLICA Y CIBERSEGURIDAD - MÉXICO

TallaPolitica - Con el objetivo de avanzar en la construcción de un marco normativo en materia de Inteligencia Artificial (IA), la Comisión de Análisis, Seguimiento y Evaluación sobre la aplicación y desarrollo de la IA en México, que preside el senador Rolando Zapata Bello, llevó a cabo el segundo conversatorio con especialistas en el rubro, bajo el tema “Roles de la IA en seguridad pública, ciberseguridad y gestión de riesgos”.

EL PRI IMPULSA REFORMA PARA BLINDAR A MÉXICO CONTRA CIBERATAQUES

Heraldo de Mexico - Ante el aumento de ataques cibernéticos, estafas digitales y robo de identidad en México, el senador del Partido Revolucionario Institucional (PRI), Alejandro Moreno Cárdenas, presentó una iniciativa para fortalecer la seguridad digital del país. El también dirigente nacional del PRI, establece la creación de una Ley General de Ciberseguridad, que regulará la protección de datos y sistemas informáticos, definiendo responsabilidades claras para el sector público y privado.

CON APROBACIÓN DE CONPES DE IA, EL PAÍS YA CUENTA CON POLÍTICA PÚBLICA PARA EL DESARROLLO DE LA INTELIGENCIA ARTIFICIAL - COLOMBIA

trendTIC - La aprobación del Conpes de Política Nacional de Inteligencia Artificial (IA) es resultado del trabajo articulado y comprometido de los Ministerios TIC y de Ciencia, Tecnología e Innovación, el Departamento Nacional de Planeación, el Departamento Administrativo de la Presidencia de la República, y los Ministerios de Comercio, Industria y Turismo; Educación y Trabajo. A través de esta Política Pública, el Estado colombiano se compromete a desarrollar acciones concretas para aprovechar esta tecnología de manera estratégica y sostenible, entendiendo que tiene el potencial de impulsar la productividad, la innovación y la toma de decisiones.

LEY MARCO DE CIBERSEGURIDAD: CÓMO Y A QUÉ EMPRESAS AFECTA - CHILE

Mala Espina - La Agencia Nacional de Ciberseguridad definirá en marzo los dos grupos que deberán seguir las obligaciones en la materia: servicios escenciales y operadores de importancia vital. Ambos grupos deberán prevenir, reportar y resolver los incidentes en ciberseguridad en sus empresas, o enfrentarán multas de hasta 40 mil UTM.

DEEPSEEK BLOQUEADA EN VARIOS PAÍSES POR RIESGOS DE CIBERSEGURIDAD

MegaNoticias - La inteligencia artificial DeepSeek, desarrollada en China, ha generado gran controversia a nivel mundial en las últimas semanas. Varios países han decidido restringir su uso debido a preocupaciones sobre la protección de datos y la seguridad nacional. Corea del Sur fue el último en sumarse a la lista este 15 de febrero, al suspender el servicio local de la aplicación por presuntas violaciones a sus leyes de privacidad.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2025

CONOCE EL NÚMERO DE LAS AMENAZAS BLOQUEADAS POR SEGUNDO: REDES SOCIALES PREFERIDAS POR ESTAFADORES

Forbes - Las redes sociales, la IA y la confianza humana provocaron un año récord de estafas avanzadas y pérdida de datos personales. El informe [Gen] revela un aumento de las amenazas en línea para cerrar un 2024 de récord, con 2.55 mil millones de ciberamenazas bloqueadas entre octubre y diciembre, lo que equivale a 321 amenazas por segundo.

ESTOS SON LOS RIESGOS A LOS QUE EXPONE SUS DATOS PERSONALES EN LAS PLATAFORMAS DIGITALES

La Republica - Uno de los mayores retos que enfrentan las nuevas generaciones digitales , tras la evolución de herramientas como la inteligencia artificial, es lograr proteger la información privada de los usuarios. Aunque la digitalización de la cotidianidad aceleró procesos de trabajo, también es cierto que puso, casi que en bandeja de plata, la información personal de los usuarios a la merced y voluntad de las empresas digitales, caldo de cultivo para posibles fraudes.

WHAT A NEW PRESIDENCY MEANS FOR GLOBAL CYBERSECURITY—AND FOR SMES - USA

Forbes - As a cybersecurity leader dedicated to safeguarding small- and medium-sized enterprises (SMEs) from cyber threats, the shifting sands of the cybersecurity landscape are always top-of-mind. The recent election of Donald Trump as President of the United States introduces new dynamics that could significantly impact global cybersecurity practices.

CYBER CONSPIRACY MODERNIZATION ACT PROPOSED, CYBER EXPERT WEIGHS IN - USA

Security Magazine - A bipartisan bill introduced by Senator Mike Rounds (R-SD) and Senator Kirsten Gillibrand (D-NY) aims to increase punishment for cybercrimes. This bill, the Cyber Conspiracy Modernization Act (CCMA), seeks to modify the Computer Fraud and Abuse Act (CFAA) in order to enact a penalty for conspiracy and strengthen penalties for offenders. This bill was introduced in as a set, joined by the Providing Individuals Various Opportunities for Technical Training to Build a Skills-Based Cyber Workforce Act of 2025 (Cyber PIVOTT Act), which would offer scholarships for students and professionals in cyber-related fields.

THE AI HYPE FRENZY IS FUELING CYBERSECURITY RISKS

Forbes - The artificial intelligence gold rush has reached a fever pitch. Companies are throwing billions—no, trillions—at AI projects, slapping the "AI-powered" label on everything from email filters to coffee makers. AI is no longer just a technology; it’s a buzzword, a marketing gimmick and a financial frenzy all rolled into one. We’ve warned about this before. AI is not magic—it’s just software with access to massive datasets, making predictions based on patterns. But the relentless hype machine has distorted reality, and now we’re facing the consequences. This unchecked AI mania is driving expected catastrophic cybersecurity risks—some of which may be irreversible.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2025

THE HIDDEN CYBERSECURITY CRISIS: HOW GENAI IS FUELING THE GROWTH OF UNCHECKED NON-HUMAN IDENTITIES

Security Boulevard - Generative AI continues its promises of revolutionizing industries and transforming everything from customer service to software development. Behind the excitement, organizations continue to struggle to identify and validate applicable use cases for GenAI that bring real business benefits. At the same time, industry leaders and social pundits continue to beat their loud revolutionary GenAI drums, enticing employees to frantically play with every new AI tool or risk losing professional and personal relevance. By doing so, they unknowingly grant access to APIs, service accounts, tokens and other NHIs which in in turn grant these applications extensive ecosystem permissions and access. As a result, a growing cybersecurity crisis is emerging — one that many organizations are unprepared to handle. GenAI is accelerating the unchecked growth of NHIs, fueling a new wave of cyberthreats.

THE FOUNDATION OF MODERN SOFTWARE DEVELOPMENT IS UNDER RISING CYBER ATTACK

NBC New York - Organizations are seeing a rise in cybersecurity attacks against application programming interfaces, and they aren't always prepared to defend themselves. As the foundation of modern software development, APIs facilitate communication between apps and fuel digital transformation, but this critical role has broadened the attack surface, making APIs a prime target for cybercriminals. The average cost to remediate API incidents was $591,400 in the U.S. In sectors such as financial services, the average was $832,800.