



INSIGHTS

JANUARY 22, 2026

DIGI AMERICAS ALLIANCE MEMBERS

Apple

aws

Batuta

CHECK POINT

CISCO

CLOUDFLARE

CROWDSTRIKE

fluid attacks
we hack your software

Google

kriptos

LUMU

MasterCard

netskope

paloalto NETWORKS

Resecurity

Schneider Electric

SISAP
Sistemas Aplicativos

SOPHOS

tenable

Trellix

TREND MICRO

LEY DE PROTECCIÓN DE DATOS EN PARAGUAY: CÓMO LA NORMA 7593 REDEFINE LA CIBERSEGURIDAD Y EL NEGOCIO DIGITAL

LexLatin - El pasado año Paraguay encabezó varias veces las noticias regionales con un tema particularmente álgido: la protección en línea. Cuando esta nación ocupó los titulares lo hizo por una razón: sus defensas contra el robo de datos y los hackeos son débiles y esto convirtió al país en un blanco fácil y recurrente de ciberpiratas que demostraron no solo la fragilidad de su sistema de protección sino la urgente necesidad de avanzar en legislaciones que cubran esta materia.

LA CIBERSEGURIDAD VUELVE A LA AGENDA PÚBLICA EN MÉXICO, EL RETO ES LA EJECUCIÓN

Cronica - Durante años, la ciberseguridad en México fue reconocida como importante, pero tratada como un tema secundario y sin continuidad en la agenda nacional. Por eso, la elaboración del Plan Nacional de Ciberseguridad 2025-2030 y de la Política General de Ciberseguridad para la Administración Pública Federal representa un cambio relevante: el Estado asume que no hay transformación digital posible sin seguridad. Ambos documentos reinsertan la ciberseguridad en la conversación pública con diagnóstico, narrativa y una ruta general. Reconocen que el entorno actual combina riesgos digitales y físicos: ciberdelincuencia organizada, tensiones geopolíticas, cadenas de suministro frágiles y el uso de inteligencia artificial para potenciar ataques.

ALERTAN REZAGOS DE MÉXICO EN CIBERSEGURIDAD Y RIESGOS PARA SU SOBERANÍA DIGITAL

msn - México enfrenta un escenario cada vez más complejo en materia de ciberseguridad, con amenazas que pueden comprometer desde la operación de instituciones públicas y empresas hasta la protección de datos personales y la soberanía digital del país. Así lo advirtieron especialistas durante el foro "Ciberseguridad: Juventud, Soberanía Digital y Tecnología", realizado en la Cámara de Diputados. En el encuentro expertos urgieron a fortalecer el marco jurídico y la capacidad de respuesta del Estado mexicano para evitar que el país siga siendo altamente vulnerable frente a ciberataques de gran escala y campañas maliciosas dirigidas contra su infraestructura crítica.

CYBERSECURITY GAPS PERSIST AS DIGITAL FRAUD ACCELERATES IN MEXICO

Mexico Business News - While Mexico advances in digital maturity, fraud remains the primary obstacle to digital trust. Although eight out of 10 users feel capable of protecting themselves online, nearly 80% faced scam attempts in the previous year, reveals the Global Cybersecurity Study 2025 by Mastercard. "Mexico is experiencing a historic acceleration in digital payments and financial services. This progress opens a strategic opportunity: to consolidate trust as the main driver of economic growth," says Marcos Peralta, Vice President, Customer Solutions Center, Mastercard North Latin America. When cybersecurity is integrated from design, innovation can scale responsibly and generate sustained value for consumers, companies, and the financial system as a whole."

PANAMÁ Y JAPÓN AVANZAN EN COOPERACIÓN SOBRE CIBERSEGURIDAD Y PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

ReporteAsia - Panamá y Japón fortalecieron su agenda de cooperación bilateral en ciberseguridad, protección de infraestructuras críticas y sectores estratégicos, durante la reunión de ciberseguridad entre los dos países, encabezada por el ministro de Relaciones Exteriores encargado, Carlos A. Hoyos, con la participación de autoridades gubernamentales y equipos técnicos de ambos países. El encuentro permitió un intercambio de criterios y experiencias sobre la protección de activos estratégicos como el Canal de Panamá, la plataforma logística nacional y proyectos de infraestructura en desarrollo, incluidos los planes de conectividad entre el Caribe y el Pacífico.

JUSTIÇA FEDERAL VAI USAR GAMIFICAÇÃO PARA TREINAR JUÍZES EM SEGURANÇA CIBERNÉTICA - BRASIL

Convergencia Digital - A Justiça Federal vai lançar ainda este ano um novo programa de capacitação voltado à segurança cibernética. A iniciativa, intitulada Exercícios de Segurança Cibernética na Justiça Federal, será promovida pela Corregedoria-Geral da Justiça Federal em parceria com o Centro de Estudos Judiciários do Conselho da Justiça Federal. A proposta parte do diagnóstico de que todo sistema informatizado, cedo ou tarde, será testado por falhas ou ofensivas externas, e que a diferença está na capacidade de resposta. Em vez de formações teóricas, o curso apostará em uma metodologia inovadora de gamificação para desenvolver competências práticas. Os participantes serão expostos a simulações colaborativas e imersivas, com atividades presenciais e a distância.

LA UE QUIERE VETAR A HUAWEI Y ZTE DE LAS REDES DE TELECOMUNICACIONES EUROPEAS POR "RIESGOS A LA DEMOCRACIA Y LA ECONOMÍA"

infobae - La Comisión Europea ha avanzado este martes en su intención de excluir de las redes de telecomunicaciones y otras infraestructuras críticas de los países miembros a proveedores extranjeros de alto riesgo como las tecnológicas chinas Huawei y ZTE, planteando que las recomendaciones de seguridad para las redes 5G que realiza Bruselas sean obligatorias. Según la mandataria, esta paquete de medidas es un paso importante para asegurar la soberanía tecnológica europea y garantizar "una seguridad mayor para todos", por lo que la UE ofrecerá todos los medios necesarios para "proteger mejor las cadenas de suministros de las infraestructuras críticas y combatir de manera decisiva del ciberataques".

LÍDERES ALERTAN EN DAVOS SOBRE LA BAJA PREPARACIÓN DE AMÉRICA LATINA FRENTE A CIBERATAQUES

EFEcomunica - Líderes de gobiernos, empresas y organismos multilaterales se reunieron en Davos para analizar el impacto de la ciberseguridad en la estabilidad económica, donde América Latina registra el nivel más bajo de confianza global para responder a un ciberataque de gran escala, con apenas un 13 %, según datos analizados en el marco del Foro Económico Mundial. En el diagnóstico, abordado durante una mesa redonda privada organizada por Digi Americas Alliance y alojada por Google Cloud, al margen del Foro Económico Mundial, los participantes coincidieron en que la ciberseguridad ha dejado de ser un asunto técnico para convertirse en pilar de competitividad, confianza digital e inclusión económica.

UK AND CHINA REACH OUT ACROSS CYBER NO-MAN'S LAND

ComputerWeekly - The British and Chinese authorities have reached out to one another to explore setting up a cyber security forum between the two countries, according to reports. The so-called 'cyber dialogue' will supposedly help to manage cyber threats to both country's national security, revealed *Bloomberg*, which was first to report the move citing anonymous sources with knowledge of the forum. It claimed that the forum will improve communication, enable private discussions and de-escalate tensions. It also establishes a direct line between London and Beijing to enable senior officials to discuss ongoing cyber incidents.

CYBER THREATS ACCELERATE GLOBALLY AS AI, GEOPOLITICS, AND FRAUD RESHAPE CYBERSECURITY LANDSCAPE

babl - Cybersecurity threats are accelerating at a global scale, driven by rapid advances in artificial intelligence, geopolitical volatility, and a sharp rise in cyber-enabled fraud, according to the World Economic Forum's "Global Cybersecurity Outlook 2026" report. The annual survey of CEOs, CISOs, and cybersecurity leaders finds that emerging technologies are expanding both attack surfaces and defensive capabilities, producing what analysts describe as a "cyber arms race." The report warns that AI has become the most significant force shaping cyber risk, with 94% of surveyed organizations identifying it as the leading driver of change in 2026. Adoption cuts both ways: organizations are deploying AI to automate detection and response, yet attackers are using the same tools to enhance phishing, reconnaissance, and social engineering. At the same time, 87% of respondents reported that AI-related vulnerabilities grew faster in 2025 than any other cyber risk, underscoring rising concerns over data exposure and adversarial capabilities.

AI VS. AI IS THE NEW SECURITY BATTLEGROUND

Fierce Network - Telcos and enterprises must prepare for emerging security threats posed by AI in the hands of attackers, part of a broader trend toward industrialized cybercrime. As the security landscape changes, the role of telcos and other communications service providers is growing. CSPs must move beyond simple connectivity to securing the entire ecosystem of 5G, AI and IT and OT technologies. Ian Swanson, Palo Alto Networks VP of AI security noted unauthorized action is eclipsing data leakage as the primary threat to organizations. "These agents require deep integration into our IT ecosystems to do their jobs. They connect directly to APIs, SaaS platforms and databases. That means a successful attack triggers real consequences."