



INSIGHTS

NOVEMBER 13, 2025

DIGI AMERICAS ALLIANCE MEMBERS



PANAMÁ | NUEVA LEY DE CIBERDELINCUENCIA OBLIGA A LAS EMPRESAS A REFORZAR SU SEGURIDAD DIGITAL

DPL News - La entrada en vigor de la Ley 478 de 2025, que actualiza el marco penal contra la ciberdelincuencia en Panamá, marca un antes y un después para las empresas del país. La norma refuerza las sanciones por delitos informáticos y modifica el Código Procesal Penal, introduciendo obligaciones inéditas para el sector privado: desde la preservación de evidencia digital hasta la colaboración obligatoria con el Ministerio Público.

BANCO CENTRAL ESTABELECE NOVAS REGRAS PARA OPERAÇÃO DE EMPRESAS DE CRIPTOATIVOS NO BRASIL

Farol da Bahia - O Banco Central (BC) anunciou nesta segunda-feira (10) a criação de um novo marco regulatório para empresas que prestam serviços com criptoativos no Brasil. As normas, que passam a valer em fevereiro de 2026, determinam que essas companhias deverão obter autorização da instituição para operar e se enquadrar como Sociedades Prestadoras de Serviços de Ativos Virtuais (SPSVAs). Segundo o BC, as SPSVAs terão nove meses, a partir da vigência da norma, para se adequar às novas exigências, que incluem regras de transparência, governança, segurança cibernética, prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo. As empresas que não comprovarem conformidade dentro do prazo não poderão continuar operando, e seus clientes terão 30 dias para transferir os ativos a instituições autorizadas.

FEBRABAN DISCUSSES CYBERSECURITY AND VIRTUAL ASSETS AT THE 15TH RISK MANAGEMENT CONGRESS - BRAZIL

Politica Distrital - The Brazilian Federation of Banks (Febraban) is scheduled to hold the 15th edition of the International Risk Management Congress (G-Risc) on November 12th and 13th, 2025, at Villa Blue Tree in São Paulo. This traditional event in the banking sector is expected to bring together authorities, experts, and executives from major financial institutions to discuss the main trends and challenges shaping the risk agenda in the country, focusing on risk culture, liquidity, virtual assets, and cyber resilience.

CIBERSEGURIDAD Y APUESTAS: EL DESAFÍO ESTRATÉGICO DEL SECTOR REGULADO EN ARGENTINA

puntobiz - El ecosistema del juego regulado en Argentina atraviesa un proceso de transformación impulsado por la digitalización de las apuestas y las loterías provinciales. Esta modernización lleva a que los operadores gestionen una enorme cantidad de datos personales, transacciones y flujos financieros. En ese contexto, la ciberseguridad deja de ser un aspecto técnico subordinado para convertirse en un factor estratégico de competitividad, reputación y confianza. Garantizar la integridad de las plataformas y la protección de la información es esencial para consolidar un modelo sostenible y con proyección regional.

LA ESCASEZ DE EXPERTOS EN CIBERSEGURIDAD FRENA LA DEFENSA DIGITAL DE LAS EMPRESAS EN MÉXICO

IT Sitio - Las empresas enfrentan un enemigo silencioso pero creciente, la falta de profesionales en ciberseguridad. Esta escasez de talento no es un tema menor se volvió un factor crítico que amenaza la continuidad operativa, la reputación corporativa y en última instancia, el desarrollo económico de las organizaciones en el país. A nivel global, la firma ISC2 estimaba en 2024 que la fuerza laboral de ciberseguridad alcanzaba los 5.5 millones de profesionales, pero el crecimiento ya limitado se estancó. Al mismo tiempo, la brecha global entre profesionales disponibles y los necesarios ronda los 4.8 millones de vacantes, de las cuales cerca de 328 397 corresponden a América Latina y, en el caso de México, se calcula que el déficit es de alrededor de 25 mil especialistas.

MEXICO'S AI EXPOSURE GAP: SECURING INNOVATION FOR ECONOMIC GROWTH

Mexico Business Review - Artificial intelligence is reshaping Mexico's economy and transforming sectors, ranging from manufacturing to finance. Companies are racing to embed AI in operations to cut costs, innovate faster, and stay competitive. Yet, cybersecurity capabilities are not keeping pace. This widening "AI exposure gap" — between innovation and protection — puts data, systems, and reputations at risk, jeopardizing the economic growth and digital trust Mexico seeks from AI. In the race to innovate, Mexico is emerging as a regional AI hub, driven by global investment and growing domestic demand.

LACNIC PRIORIZA TRANSPARENCIA, EFICIENCIA INTERNA Y CIBERSEGURIDAD EN PLAN ESTRATÉGICO

DPL News - El Plan Estratégico 2026-2029 de Lacnic dará continuidad a las acciones que la organización ha venido realizando durante las poco más de dos décadas que tiene de existencia y contempla cinco prioridades, contó su director ejecutivo, Ernesto Majó. El nuevo plan estratégico contempla 5 ejes: 1. Trabajo con la comunidad de LACNIC 2. Construcción de capacidades técnicas 3. Eficiencia interna 4. Fortalecimiento de la transparencia y 5. Seguridad de la información. La Inteligencia Artificial es un fenómeno disruptivo, más que emergente, y tiene dos lados, uno positivo, estamos tratando de aprovecharla e incorporarla en diferentes procesos que nos permitan ser más productivos, más eficientes y brindar mejores servicios; el más difícil tiene que ver con las implicancias de ciberseguridad", comentó Majó a propósito del impacto de la IA en el ámbito del Internet.

TENDENCIAS EN CIBERSEGURIDAD OFENSIVA Y DEFENSIVA

Impacto TIC - A pesar de los avances tecnológicos, las ciberamenazas en América Latina siguen en aumento, ahora potenciadas con nuevas herramientas tecnológicas, para hacerles frente una estrategia es pasar de la ciberseguridad ofensiva a la defensiva, ¿pero en qué consiste esta tendencia y qué beneficios trae a las empresas? Para 2026, las tendencias en ciberseguridad estarán dominadas por una 'carrera armamentista de IA', donde tanto atacantes como defensores usarán la Inteligencia Artificial. Este enfoque vuelve obsoletos a los modelos tradicionales y obligará a las empresas a adoptar estrategias integradas de ciberseguridad ofensiva y defensiva. Se trata de un enfoque más relevante que nunca cuando consideramos que entre agosto de 2024 y junio de 2025 se registraron más de 3,1 millones de ciberataques diarios en América Latina, con Colombia dentro del top 5 regional y un crecimiento sostenido frente a 2023.

CÓMO AFECTA A LAS EMPRESAS EL DÉFICIT EN ESPECIALISTAS EN CIBERSEGURIDAD

E&N - El déficit de talento en ciberseguridad se ha convertido en un factor crítico que pone en riesgo el funcionamiento continuo de las empresas, tanto en América Latina como en el resto del mundo. Según datos del Estudio de la fuerza laboral de ciberseguridad de ISC2 de 2024, la fuerza laboral global ha alcanzado una cifra de 5.5 millones de profesionales, pero este crecimiento se ha estancado. Al mismo tiempo, la brecha global de especialistas en ciberseguridad, es decir, la diferencia entre el número de profesionales capacitados disponibles y el número necesario para proteger los sistemas empresariales; ha llegado a cerca de 4.8 millones de puestos vacantes, de los cuales en América Latina se identifica una escasez de 328,397 especialistas, en México, se calcula que el déficit es de 25.000 profesionales.

DEPARTMENT OF WAR INTRODUCES NEW CYBERSECURITY RISK MANAGEMENT FRAMEWORK - USA

Federal Newswire - The Department of War (DoW) has announced the launch of a new Cybersecurity Risk Management Construct (CSRMC), designed to provide real-time cyber defense for U.S. military operations. The CSRMC aims to address shortcomings in the previous risk management framework, which relied on static checklists and manual processes that did not adequately support operational needs or cyber survivability. These limitations left defense systems open to advanced threats and delayed the deployment of secure capabilities.

WHY LITHUANIA IS EUROPE'S CYBERSECURITY CHAMPION FOR DATA CENTERS

Data Center Dynamics - Data centers store and process vast amounts of sensitive data, making them prime targets for cyber threats. As cyber attacks grow more frequent and sophisticated, data centers need more than just infrastructure – high cybersecurity levels are now essential for their protection and resilience. Lithuania delivers exactly that – the country is a known cybersecurity leader that combines well-developed digital connectivity, reliable power supply, and a skilled talent pool. Lithuania consistently ranks among the top cybersecurity locations globally. In 2025, the country was recognized as 1st in Europe and 3rd globally for cybersecurity performance by StartupBlink, a global startup research platform.