



INSIGHTS

MARCH 5, 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

TrendAI

MINTIC ACTIVA PLAN NACIONAL DE CIBERSEGURIDAD Y COMUNICACIONES PARA GARANTIZAR LA ESTABILIDAD TECNOLÓGICA EN LAS ELECCIONES DEL 8 DE MARZO - COLOMBIA

MinTIC.gov.co - De cara a las elecciones legislativas del próximo 8 de marzo, jornada que también incluirá tres consultas, el Ministerio de Tecnologías de la Información y las Comunicaciones consolidó el alistamiento técnico y operativo para garantizar la estabilidad de las redes, la seguridad digital y la continuidad de los sistemas que respaldan el proceso electoral.

COLOMBIA Y REINO UNIDO FORTALECEN DIÁLOGO ESTRATÉGICO EN MATERIA DE CIBERSEGURIDAD

Cancilleria.gov.co - Colombia y el Reino Unido llevaron a cabo una Mesa Redonda sobre Amenazas Cibernéticas con el objetivo de fortalecer el diálogo estratégico y la cooperación bilateral en materia de ciberseguridad. La iniciativa fue impulsada por el Ministerio de Relaciones Exteriores, a través de la Dirección de Asuntos Políticos Multilaterales, tras identificar necesidades específicas de fortalecimiento de capacidades frente a amenazas emergentes en el entorno digital, así como oportunidades de cooperación con socios estratégicos.

LEY MARCO DE CIBERSEGURIDAD DE CHILE Y LA NECESIDAD DE INTERNALIZAR LOS DESAFÍOS, DIRECTRICES Y SU EFICIENTE CUMPLIMIENTO

trendTIC - En Chile, los ciberataques dejaron de ser incidentes aislados para convertirse en una amenaza sistémica. Pero, ya las empresas no tendrán que enfrentar estas situaciones solas. En el país se promulgó la Ley Marco de Ciberseguridad, que también impulsó la creación de la Agencia Nacional de Ciberseguridad (ANCI). A través de ellas el Estado busca establecer normativas para proteger la seguridad digital del país, crear un ecosistema seguro, fomentar una cultura de ciberseguridad y regular a organismos públicos y privados en la materia.

CNJ MUDA REGRAS E EXIGE PADRÕES MÍNIMOS DE SEGURANÇA DIGITAL E TI EM 12 MIL CARTÓRIOS - BRASIL

Convergencia Digital - Mais de 12 mil cartórios terão de reforçar a infraestrutura tecnológica e mecanismos de segurança digital por conta de novas regras do Conselho Nacional de Justiça. A norma estabelece padrões nacionais mínimos de tecnologia da informação e governança de dados para os serviços notariais e de registro, com impacto direto na operação das serventias em todo o país. Segundo o CNJ, a medida busca elevar o nível de proteção dos sistemas que armazenam informações sensíveis de cidadãos e empresas, além de garantir maior continuidade dos serviços digitais prestados pelos cartórios. Na prática, o provimento exige que as serventias adotem políticas formais de segurança da informação, controles mais rigorosos de acesso aos sistemas e procedimentos estruturados de resposta a incidentes cibernéticos.

REDUCIR CIBERATAQUES PODRÍA AUMENTAR EL PIB EN PAÍSES EN DESARROLLO, SEGÚN INFORME DEL BANCO MUNDIAL

El Jaya - Durante el mismo encuentro, representantes de ANATEL y del Caribbean Digital Transformation Project destacaron los principales desafíos que enfrenta América Latina en materia de ciberseguridad y transformación digital. Entre ellos, señalaron la lentitud normativa frente al acelerado avance de la digitalización, así como la escasez de personal especializado en tecnologías digitales, una situación agravada por restricciones presupuestarias en el sector público. Como parte de las recomendaciones estratégicas para fortalecer la seguridad digital en la región, propusieron aprovechar infraestructuras administrativas ya existentes, coordinar políticas de ciberseguridad en sectores críticos —como energía, finanzas y telecomunicaciones— y estandarizar las normativas sobre protección de datos y ciberdelincuencia.

CIBERRESILIENCIA NACIONAL EN LA ERA DE LA INTELIGENCIA ARTIFICIAL

Prensario TI Latin America - Durante años, la ciberseguridad fue considerada un asunto técnico. Un tema que vivía en los centros de datos y en los equipos de TI. Hoy esa visión quedó atrás. La seguridad digital impacta directamente la continuidad operativa del Estado, la estabilidad económica y la confianza pública. Lo que cambió no es solo la cantidad de ataques, sino su sofisticación y propósito. Los adversarios ya no buscan únicamente robar información. Se infiltran, permanecen ocultos durante largos períodos y esperan el momento oportuno para generar disrupción. Las cifras lo demuestran. Según el más reciente reporte global de Check Point, en 2025 las organizaciones enfrentaron en promedio 1.968 ciberataques semanales a nivel mundial, un 18% más que el año anterior. En Chile, la presión es igualmente significativa: actualmente las organizaciones chilenas registran en promedio 1.846 ciberataques por semana, lo que representa un aumento de 9% en comparación con el año previo.

LEAKBASE CYBERCRIME FORUM SHUT DOWN, SUSPECTS ARRESTED

Security Week - LeakBase had been active since 2021 and in December 2025 it had roughly 142,000 registered users, who sold and bought stolen information, including account credentials, personally identifiable information, payment card data, and bank account details. As part of Operation Leak, law enforcement shut down two domains used by the forum and seized the LeakBase database. Seizure of the database enabled the identification of 'multiple' users. Evidence collected by investigators included user account details, forum posts, private messages, and IP logs. Europol said the forum had approximately 215,000 private messages and 32,000 posts.

LATAM NOW FACES 2X MORE CYBERATTACKS THAN US

Dark Reading - Nowhere in the world has cyber threat activity been growing faster than in Latin America, thanks in part to relatively rapid digital adoption on the part of businesses in the region, combined with relatively stagnant cybersecurity growth. Last year, researchers at Check Point tracked a 53% year-over-year rise in weekly cyberattacks in Latin America, and as of 2026, they confirmed it to be the most heavily targeted region on the planet. In an updated, unpublished March 2026 threat report shared with Dark Reading, Check Point found that Latin American organizations currently face an average of around 3,100 cyber threats per week. By comparison, in recent months, their counterparts in the United States have averaged just under 1,500.

WHY THE CORE OF MODERN CYBERSECURITY IS BRIDGING IDENTITY AND DATA

Forbes - AI is no longer something organizations are experimenting with at the edges. It's threading itself into the everyday machinery of business. According to my company's March 2025 survey of 2,150 IT professionals from 121 countries, "60% of organizations are already leveraging AI tools in their IT infrastructures." At the same time, AI adoption is also occurring outside formal IT programs, often without visibility or governance. Not surprisingly, AI is a topic in nearly every security conversation I'm having with customers. One CISO admitted they discovered access paths in their environment that they didn't even know existed. Another customer shared, "We didn't realize how much our identity model was held together by duct tape until AI started pulling on it."

WHY CYBERSECURITY IS NOW A STRATEGIC IMPERATIVE FOR BUSINESS GROWTH, TRUST AND RESILIENCE

World Economic Forum - Cyber incidents now quickly become a leadership problem. Cyber incidents have impacts on operations, the balance sheet and the trust that keeps customers and partners leaning in. Yet too many organizations still treat cybersecurity as a technical function or a compliance hurdle. That misalignment is becoming harder to defend as geopolitics, regulation, supply-chain interdependence, cybercrime and emerging technologies increase the complexity of the cyber landscape. Cybersecurity is now therefore a core business imperative. The chief information security officer (CISO) sits at the centre of that complexity and its role is increasingly strategic.

STRENGTHENING NORTH AMERICA'S DIGITAL COMPETITIVENESS THROUGH CYBERSECURITY AND SME INCLUSION

Brookings - The 2026 review of the United States–Mexico–Canada Agreement (USMCA) presents a critical opportunity to strengthen North America's digital competitiveness, modernize Chapter 19 (Digital Trade), and reinforce regional cooperation on cybersecurity, artificial intelligence (AI), data governance, and small- and medium-sized enterprise (SME) inclusion. North America is undergoing rapid technological transformation driven by AI, cloud services, automation, cybersecurity needs, and digital trade. While the digital economy has become a major engine of growth—exceeding \$1.5 trillion in cross-border digital trade—SMEs continue to face structural barriers such as limited access to capital, digital skills gaps, and regulatory fragmentation.