DIGI AMERICAS ALLIANCE MEMBERS

Apple aws Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE
fluid attacks we hack your software Google kriptos LUMU netskope paloalto NETWORKS
Resecurity Schneider Electric SISAP Sistemas Aplicativos SOPHOS tenable Trellix TrendAI

MINTIC ACTIVATES NATIONAL CYBERSECURITY AND COMMUNICATIONS PLAN TO GUARANTEE TECHNOLOGICAL STABILITY IN THE MARCH 8 ELECTIONS - COLOMBIA

MinTIC.gov.co - In preparation for the legislative elections on March 8, which will also include three referendums, the Ministry of Information and Communications Technologies has finalized the technical and operational readiness to guarantee network stability, digital security, and the continuity of the systems that support the electoral process.

COLOMBIA AND THE UNITED KINGDOM STRENGTHEN STRATEGIC DIALOGUE ON CYBERSECURITY

Cancilleria.gov.co - Colombia and the United Kingdom held a Roundtable on Cyber Threats to strengthen strategic dialogue and bilateral cooperation on cybersecurity. The initiative was spearheaded by the Ministry of Foreign Affairs, through its Directorate of Multilateral Political Affairs, after identifying specific needs for capacity building in the face of emerging threats in the digital environment, as well as opportunities for cooperation with strategic partners.

CHILE'S CYBERSECURITY FRAMEWORK LAW AND THE NEED TO INTERNALIZE THE CHALLENGES, GUIDELINES AND ITS EFFICIENT COMPLIANCE

trendTIC - In Chile, cyberattacks have gone from being isolated incidents to a systemic threat. But companies will no longer have to face these situations alone. The country enacted the Cybersecurity Framework Law, which also led to the creation of the National Cybersecurity Agency (ANCI). Through these laws, the State seeks to establish regulations to protect the country's digital security, create a secure ecosystem, foster a cybersecurity culture, and regulate public and private organizations in this area.

CNJ CHANGES RULES AND REQUIRES MINIMUM STANDARDS FOR DIGITAL SECURITY AND IT IN 12,000 NOTARY OFFICES - BRAZIL

Digital Convergence - More than 12,000 notary offices will have to reinforce their technological infrastructure and digital security mechanisms due to new rules from the National Council of Justice (CNJ). The regulation establishes minimum national standards for information technology and data governance for notarial and registry services, with a direct impact on the operation of these offices throughout the country. According to the CNJ, the measure seeks to raise the level of protection of systems that store sensitive information of citizens and companies, in addition to ensuring greater continuity of digital services provided by notary offices.

REDUCING CYBERATTACKS COULD INCREASE GDP IN DEVELOPING COUNTRIES, ACCORDING TO A WORLD BANK REPORT

El Jaya – During the same meeting, representatives from ANATEL and the Caribbean Digital Transformation Project highlighted the main challenges facing Latin America in cybersecurity and digital transformation. Among these, they pointed to the slow pace of regulatory development in the face of rapid digitalization, as well as the shortage of personnel specializing in digital technologies, a situation exacerbated by budget constraints in the public sector. As part of their strategic recommendations to strengthen digital security in the region, they proposed leveraging existing administrative infrastructure, coordinating cybersecurity policies in critical sectors—such as energy, finance, and telecommunications—and standardizing regulations on data protection and cybercrime.

NATIONAL CYBER RESILIENCE IN THE AGE OF ARTIFICIAL INTELLIGENCE

Prensario TI Latin America - For years, cybersecurity was considered a technical matter, confined to data centers and IT teams. Today, that view is outdated. Digital security directly impacts government operational continuity, economic stability, and public trust. What has changed is not only the number of attacks, but also their sophistication and purpose. Adversaries no longer seek only to steal information. They infiltrate, remain hidden for extended periods, and wait for the opportune moment to cause disruption. The figures prove it. According to Check Point's most recent global report, in 2025 organizations faced an average of 1,968 cyberattacks per week worldwide, 18% more than the previous year. In Chile, the pressure is equally significant: Chilean organizations currently register an average of 1,846 cyberattacks per week.

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.