DIGI AMERICAS ALLIANCE MEMBERS

Apple AppGate aws Batuta Chainguard CHECK POINT CISCO CLOUDFLARE
CROWDSTRIKE fluidattacks Google kriptos LUMU netskope paloalto NETWORKS Schneider Electric
SISAP Sistemas Aplicativos SOPHOS TANIUM tenable Trellix TrendAI whalemate zscaler

BANKING AND TELECOMMUNICATIONS SEE OPPORTUNITIES IN PANAMA'S AI STRATEGY

La Estrella de Panamá – The presentation of the National Artificial Intelligence (AI) Strategy by Senacyt (the National Secretariat of Science, Technology and Innovation) generated broad support in the Panamanian private sector. Voices from the banking, telecommunications, and cybersecurity sectors agree that the country has a unique opportunity to consolidate itself as a digital hub in the Americas, complementing its logistical and financial role. The telecommunications sector cautioned that AI is both an opportunity and a threat: Panama's cybersecurity maturity is around 46%, while the banking sector reaches approximately 65%, gaps that still need to be closed by strengthening data governance and the protection of sensitive information.

PANAMA IS ANALYZING MECHANISMS TO APPLY ITBMS TO DIGITAL SERVICES

AIG - The general administrator of the National Authority for Government Innovation (AIG), Adolfo Fábrega, explained the scope of the initiative that seeks to apply the 7% ITBMS (Transfer Tax on Movable Goods and Services) to certain digital services used in Panama. The proposal aims to establish a more equitable playing field between businesses established in the country and international platforms that offer digital services to local consumers, such as streaming platforms, music services, productivity tools, email, and other cloud-based corporate services. Ideally, the platforms themselves would incorporate the 7% tax into their invoices and remit the tax to the Panamanian treasury; as an alternative, a mechanism using electronic payment methods, in coordination with banking institutions, is being analyzed.

ANCI PRESENTS EXECUTIVE SUMMARY OF THE PUBLIC CONSULTATION ON CYBERSECURITY BASICS REGULATIONS - CHILE

ANCI – The Cybersecurity Framework Law establishes that, before issuing new security measures, the National Cybersecurity Agency (ANCI) must submit them to public consultation. Therefore, in June, it conducted a public consultation on six controls that ANCI refers to as the “9 Basics of Cybersecurity.” The results, based on input from hundreds of citizens, are summarized in a downloadable PDF document available on the Agency's website.

DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 27, 2026

ENTEL PROMOTES A NATIONAL AGENDA FOR BOLIVIA TO STRENGTHEN CYBERSECURITY

MOPSV - Protecting information and digital systems has become a priority for governments, businesses, and citizens worldwide. In this context, the Minister of Public Works, Mauricio Zamora, is promoting initiatives to help Bolivia advance in developing a national cybersecurity agenda. Along these lines, Entel presented the "Bolivia Cybersecure 2026" project, a forum that brought together specialists, public and private sector institutions, and national and international experts to strengthen the country's capabilities in the face of risks and threats in the digital environment. The state-owned company contributes connectivity, infrastructure, and security solutions. "Cybersecurity must be addressed as a national agenda, built on cooperation and institutional synergy," stated Entel's General Manager, Jorge Del Solar.

MINISTER VILLATE DETAILS THE PROJECTION OF TECHNOLOGICAL SOVEREIGNTY AND THE STRENGTHENING OF CYBERSECURITY - PARAGUAY

MITIC – The Minister of Information and Communication Technologies, Gustavo Villate, outlined the country's plans for technological sovereignty and the strengthening of cybersecurity. To coordinate technological development, the government is moving forward with the creation of the Innova District, a technology park focused entirely on the digital sphere that will integrate scientific research, academia, and the public and private sectors. Regarding cybersecurity, the digital security structure is divided into cyber defense, under the Ministry of Defense, and the civilian, public, and private sectors, managed by the General Directorate of Cybersecurity within MITIC. Its Computer Emergency Response Team (CERT) has transitioned to operating under a continuous 24/7 monitoring system.

ANPD EVALUATES HOW DIGITAL PLATFORMS ARE WORKING TO PREVENT CRIMINAL CONTENT AND PROTECT CHILDREN AND WOMEN ONLINE - BRAZIL

gov.br - The National Data Protection Agency (ANPD) has begun monitoring the main digital platforms, app stores, and generative Artificial Intelligence tools to verify whether they are adopting measures to comply with the obligations established by the Brazilian Civil Rights Framework for the Internet and the Digital Statute for Children and Adolescents (ECA Digital). Companies have begun to be notified and must respond within ten business days. The objective is to verify whether the platforms adopt adequate mechanisms to prevent and impede the circulation of criminal or illicit content, with special attention to risks that impact children, adolescents, and women in the digital environment.

CRC PUBLISHES STUDY ON CYBERSECURITY IN THE AGE OF AI AND PRESENTS ROADMAP FOR THE TELECOMMUNICATIONS SECTOR - COLOMBIA

The Communications Regulatory Commission (CRC) published the study “Cybersecurity in the Age of AI: Strategic Priorities and Roadmap for the Telecommunications Sector,” a comprehensive guide aimed at strengthening the digital resilience of communications networks in Colombia and understanding the emerging risks associated with artificial intelligence. The report addresses the threat landscape through five strategic pillars: the dual crisis of AI, critical infrastructure, quantum security, cyberculture, and cybersecurity training. It also includes a roadmap to international frameworks and standards for network and service providers.

DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 27, 2026

THE US DISMANTLED A CHINESE CYBERESPIONAGE NETWORK THAT TARGETED NASA, THE FEDERAL RESERVE, AND THE SENATE

Yahoo News – The U.S. Department of Justice and the FBI announced the seizure of web domains linked to two complementary hacking platforms, known as QScan and QTRouter. According to Washington, these platforms were created by a group backed by the Chinese government and used in cyberattacks against NASA, the Federal Reserve, the Senate, and multiple U.S. executive branches. The investigation revealed that QScan was used to scan and infect thousands of IoT devices, while the provider QTFY offered cyberattack services to clients linked to the Chinese Ministry of State Security and the People's Liberation Army since at least 2018.

A TALE OF TWO SOCS: INSIGHTS FROM TWO RED TEAM ASSESSMENTS - USA

CISA - The Cybersecurity and Infrastructure Security Agency conducted two simultaneous red team assessments of critical infrastructure organizations using similar tradecraft, but observed sharply different defensive outcomes. In one organization the team gained access to multiple workstations, elevated privileges over the domain and moved laterally to sensitive business systems and cloud resources undetected, while in the second, defenders quickly detected the initial compromise and quarantined the affected systems. CISA attributes the difference to factors such as alert triage, shared visibility across security tools, and hardened Active Directory, cloud token and endpoint-management controls, and urges critical infrastructure organizations to apply the advisory's mitigations.

INTERPOL CRACKS DOWN ON GLOBAL CYBER FRAUD AND MONEY LAUNDERING BY WEST AFRICAN ORGANIZED CRIME

Digital Shield – A coordinated international police operation dealt a severe blow to major organized crime networks originating in West Africa. Conducted between November 2025 and June 2026 under the name Operation Jackal IV, the initiative involved law enforcement agencies from 22 countries and resulted in 58 arrests—including 17 in Argentina—and the identification of 263 suspects, after dismantling networks dedicated to cryptocurrency fraud, romance scams, corporate email compromise, and money laundering linked to organizations such as Black Axe.

CHINESE HACKERS DOUBLED THEIR CYBERATTACKS AFTER INTEGRATING DEEPSEEK INTO THEIR OPERATIONS

Infobae - Hacker groups linked to the Chinese regime have more than doubled the volume of their cyberattacks since incorporating DeepSeek and other open-source artificial intelligence models into their operations, according to a report by the Taiwanese firm TeamT5, which tracked the use of these tools at different stages of intrusion campaigns. Researchers agreed that DeepSeek has become the preferred option for Chinese hackers due to its high performance, low operating costs, and more permissive security controls than its competitors, giving them much greater leeway than Western models.