DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 10, 2026

DIGI AMERICAS ALLIANCE MEMBERS

PROSECUTOR'S OFFICE REPORTS MORE THAN 93,000 INVESTIGATIONS AND ADVANCES IN CYBERSECURITY DURING 2025 - ECUADOR

El Norte - Acting Attorney General Leonardo Alarcón presented the accountability report for the institution's 2025 activities in a virtual event held in compliance with the provisions of the Council for Citizen Participation and Social Control. The presentation included data on coverage, resources, and actions carried out during the period.

ITLA AND THE NATIONAL POLICE STRENGTHEN COOPERATION TO COMBAT CYBERCRIME - DOMINICAN REPUBLIC

Acento – The Technological Institute of the Americas (ITLA) and the National Police of the Dominican Republic strengthened their inter-institutional cooperation with the goal of promoting training and technological development to combat cybercrime in the country. ITLA Rector Jimmy Rosario Bernard paid an official visit to General Edgar Arnaud Volquez, commander of the Cyber Police unit, to learn about the operational and technological capabilities of the specialized unit for investigating computer crimes.

COSTA RICA REGISTERED MORE THAN 40,000 REPORTS OF CYBERCRIMES IN 7 YEARS

Diario Extra - A total of 40,457 reports of cybercrimes registered between 2018 and August 2025 reflect the accelerated growth of cybercrime in Costa Rica. Between 2023 and 2024 alone, cases nearly doubled, with a 96.7% increase. This data comes from the report "State of Cybersecurity in Costa Rica 2025," prepared by the National University (UNA), which warns that "more than 40,000 reports of cybercrimes have been registered, with exponential growth that demonstrates the consolidation of cybercrime as a structural problem."

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 10, 2026

THEY SEEK TO STRENGTHEN DIGITAL SECURITY FOR MINORS IN MEXICO

Reporte Indigo – Federal Deputy Julio Scherer Pareyón led a meeting with international organizations, specialists, and the company Meta Platforms to promote a national agenda focused on strengthening the digital security of children and adolescents. During the meeting, participants agreed on the urgent need to address risks in digital environments through coordinated actions between government, civil society, academia, and technology platforms.

CLAUDE MYTHOS, THE AI THAT DETECTED THOUSANDS OF CRITICAL SOFTWARE FLAWS, WILL NOT BE LAUNCHED DUE TO CYBERSECURITY RISKS

LAFM - The technology company Anthropic decided not to release its new artificial intelligence model, called Claude Mythos, to the public after discovering its ability to detect and exploit unpatched software vulnerabilities. According to the company, the system identified thousands of flaws in commonly used applications, some of which had gone undetected for decades. This level of capability led the company to limit its use to controlled environments due to the risk it poses to digital security.

AI AND CYBERSECURITY: PROJECT GLASSWING, THE ALLIANCE OF GIANTS TO STOP IMPOSSIBLE ATTACKS

Urgente24 - How an alliance between Anthropic, Google, and Microsoft seeks to get ahead of the cybersecurity problem: an AI that can already detect vulnerabilities before many experts. The race to develop the most powerful artificial intelligence has just opened an unexpected front: cybersecurity. The company Anthropic announced the launch of Project Glasswing, an initiative that brings together tech giants like Apple, Google, Microsoft, and Amazon Web Services with a common goal: to prevent AI itself from becoming a difficult-to-control threat.

LESS THAN HALF OF PUBLIC BODIES ARE PREPARED FOR A TECHNOLOGICAL CRISIS

el destape – business continuity has ceased to be an exceptional scenario and has become a daily challenge for companies and public organizations. Power outages during peak demand, intense storms, and systems pushed to their limits expose a stark reality: without robust technological infrastructure, maintaining critical services without interruption is increasingly difficult. The problem is that preparedness is still lacking. According to a Splunk study, only 42% of public organizations consider themselves well-prepared in terms of digital resilience. Even so, the global trend indicates a shift: 65.5% of organizations have already increased their investment in business continuity, while 45.4% have a dedicated person responsible for this who reports to the board of directors.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 10, 2026

TAIWAN, US HOLD CYBERSECURITY TRAINING EVENT IN GUATEMALA

Taiwan News - Taiwan and the US held a cybersecurity training event in Guatemala for the first time, the Ministry of Foreign Affairs said Thursday. The April 6 program was held under the Global Cooperation and Training Framework. More than 100 digital experts, Guatemalan government officials, and representatives from the embassies of Taiwan and the US discussed the theme of “Strengthening Cybersecurity Resilience and Digital Infrastructure.” Participants shared practical experience on the risks of low-cost electronic products, the development of basic digital infrastructure, and regional cooperation, the ministry said in a statement. Taiwan Ambassador Vivia Chang (張俊菲) said that as Taiwan stands at the forefront of cybersecurity, it possesses both practical experience and scientific innovation capabilities.

CIA DIRECTOR QUIETLY ELEVATED AGENCY’S CYBER ESPIONAGE DIVISION - USA

The Record - The CIA late last year raised the status of its elite cyber espionage division, providing it more resources to analyze and disrupt digital threats, as well as amp up the agency’s own technological innovation efforts. The Center for Cyber Intelligence, which had resided within the CIA's Directorate of Digital Innovation since 2015, was promoted to a full-fledged mission center last October by Director John Ratcliffe as part of an internal reorganization. Ratcliffe elevated the center to “strengthen the Agency’s cyber operations in support of the president’s priorities,” Liz Lyons, a CIA spokeswoman, said in a statement.

FEDERAL BUREAU OF INVESTIGATION INTERNET CRIME REPORT 2025 - USA

FBI - In 2025, losses reported to IC3 continued to climb, surpassing the $20 billion mark. Investment-related fraud was once again the largest component of these losses, followed by business email compromises and tech support scams. The FBI continues to disrupt and deter malicious cyber actors -- and shift the cost from victims to our adversaries. One example was Operation Level Up, which countered crypto investment scams. This FBI-led initiative has reduced potential losses by more than $500 million since 2024.

TREASURY DEPARTMENT ANNOUNCES CRYPTO INDUSTRY CYBER THREAT SHARING INITIATIVE - USA

The Record - The U.S. Treasury Department said it will now share cyber threat intelligence with the cryptocurrency industry following multiple incidents where millions worth of consumer funds were stolen. Treasury’s Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) announced the initiative on Thursday, writing in a statement that they will “provide timely, actionable cybersecurity information to eligible U.S. digital asset firms and industry organizations, helping them better identify, prevent, and respond to cyber threats targeting their customers and networks.”

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 10, 2026

THE EVOLVING IRANIAN CYBER THREAT

American Security Project - The crisis in the Middle East has gripped global attention, but one front is overlooked: cyberspace. While Iranian state-operated hacking groups face reduced capacity, Tehran-allied hackers are carrying out a high number of low-to-medium sophistication attacks on critical infrastructure. Tehran is also bolstering its future cyber capabilities by increasing coordination between state-controlled groups, expanding their infrastructure, and adopting advanced tactics, techniques, and procedures (TTPs). Washington should address the immediate cyber threat by temporarily reallocating resources to train U.S. and Middle Eastern critical infrastructure providers on Iranian TTPs. Long term, Washington should reinvigorate public-private communication on cybersecurity, implement requirements on critical infrastructure cybersecurity reporting, and encourage interagency intelligence collaboration on Iranian cyber capabilities.

UNDERSTANDING CURRENT THREATS TO KUBERNETES ENVIRONMENTS

Palo Alto Networks Unit 42 - The rapid adoption of container orchestration has positioned Kubernetes as a high-value target for adversaries seeking to compromise enterprise-scale environments. Our telemetry reveals that Kubernetes-related threat actor operations, including stealing Kubernetes tokens, increased 282% over the last year. The IT sector was the most heavily targeted, representing over 78% of observed activity. We look beyond traditional container escape scenarios, and demonstrate how high-profile threat actors abuse Kubernetes identities and exposed attack surfaces to escalate privileges, pivoting from initial access to sensitive backend cloud infrastructure. Using two real-world case studies, we break down the mechanics of these attacks and the tradecraft that made them possible.

A.I. IS ON ITS WAY TO UPENDING CYBERSECURITY

The New York Times - Anthropic said late last year that state-sponsored Chinese hackers had used its artificial intelligence technology in an effort to infiltrate the computer systems of roughly 30 companies and government agencies around the world. In a blog post, Anthropic said it was the first reported case of a cyberattack in which A.I. technologies had gathered sensitive information with limited help from human operators. Human hackers, the company said, handled about 10 to 20 percent of the work needed to conduct the attack.

CLOUDFLARE TARGETS 2029 FOR FULL POST-QUANTUM SECURITY

Cloudflare - Cloudflare is accelerating its post-quantum roadmap. We now target 2029 to be fully post-quantum (PQ) secure including, crucially, post-quantum authentication. At Cloudflare, we believe in making the Internet private and secure by default. We started by offering free universal SSL certificates in 2014, began preparing our post-quantum migration in 2019, and enabled post-quantum encryption for all websites and APIs in 2022, mitigating harvest-now/decrypt-later attacks. While we're excited by the fact that over 65% of human traffic to Cloudflare is post-quantum encrypted, our work is not done until authentication is also upgraded. Credible new research and rapid industry developments suggest that the deadline to migrate is much sooner than expected. This is a challenge that any organization must treat with urgency, which is why we're expediting our own internal Q-Day readiness timeline.