DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 10, 2026

DIGI AMERICAS ALLIANCE MEMBERS

FISCALÍA REPORTA MÁS DE 93.000 DILIGENCIAS Y AVANCES EN CIBERSEGURIDAD DURANTE 2025 - ECUADOR

El Norte - El fiscal general del Estado (e), Leonardo Alarcón, presentó el informe de rendición de cuentas correspondiente a la gestión institucional de 2025, en un acto telemático realizado en cumplimiento de disposiciones del Consejo de Participación Ciudadana y Control Social. La exposición incluyó datos sobre cobertura, recursos y acciones ejecutadas durante el periodo.

ITLA Y POLICÍA NACIONAL REFUERZAN COOPERACIÓN PARA COMBATIR EL CIBERDELITO - REPÚBLICA DOMINICANA

Acento - El Instituto Tecnológico de las Américas (ITLA) y la Policía Nacional de la República Dominicana fortalecieron su cooperación interinstitucional con el objetivo de impulsar la capacitación y el desarrollo tecnológico para enfrentar los delitos electrónicos en el país. El rector del ITLA, Jimmy Rosario Bernard, realizó una visita oficial al general Edgar Arnaud Volquez, comandante del área de Policía Cibernética, con el propósito de conocer las capacidades operativas y tecnológicas de la unidad especializada en la investigación de delitos informáticos.

PAÍS REGISTRÓ MÁS DE 40 MIL DENUNCIAS POR DELITOS INFORMÁTICOS EN 7 AÑOS - COSTA RICA

Diario Extra - Un total de 40.457 denuncias por delitos informáticos registradas entre 2018 y agosto de 2025 reflejan el crecimiento acelerado del cibercrimen en Costa Rica. Solo entre 2023 y 2024, los casos casi se duplicaron, con un aumento del 96,7%. El dato se desprende del informe Estado de la Ciberseguridad en Costa Rica 2025, elaborado por la Universidad Nacional (UNA), el cual advierte que “se han registrado más de 40.000 denuncias por delitos informáticos, con un crecimiento exponencial que evidencia la consolidación de la cibercriminalidad como un problema estructural”.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 10, 2026

BUSCAN REFORZAR SEGURIDAD DIGITAL DE MENORES EN MÉXICO

Reporte Indigo - El diputado federal Julio Scherer Pareyón encabezó un encuentro con organismos internacionales, especialistas y la empresa Meta Platforms para impulsar una agenda nacional enfocada en fortalecer la seguridad digital de niñas, niños y adolescentes. Durante la reunión, los participantes coincidieron en la urgencia de atender los riesgos en entornos digitales mediante acciones coordinadas entre gobierno, sociedad civil, academia y plataformas tecnológicas.

CLAUDE MYTHOS, LA IA QUE DETECTÓ MILES DE FALLAS CRÍTICAS EN SOFTWARE, NO SERÁ LANZADA POR RIESGOS EN CIBERSEGURIDAD

LAFM - La empresa tecnológica Anthropic decidió no lanzar al público su nuevo modelo de inteligencia artificial, llamado Claude Mythos, tras comprobar que tiene la capacidad de detectar y explotar vulnerabilidades en software que no cuentan con solución. Según explicó la compañía, el sistema logró identificar miles de fallas en aplicaciones de uso común, algunas de ellas con décadas sin ser detectadas. Este nivel de capacidad llevó a la empresa a limitar su uso a entornos controlados por el riesgo que representa para la seguridad digital.

IA Y CIBERSEGURIDAD: PROJECT GLASSWING, LA ALIANZA DE LOS GIGANTES PARA FRENAR ATAQUES IMPOSIBLES

Urgente24 - Cómo una alianza entre Anthropic, Google y Microsoft busca adelantarse al problema de la ciberseguridad: una IA que ya puede detectar vulnerabilidades antes que muchos expertos. La carrera por desarrollar inteligencia artificial más potente acaba de abrir un frente inesperado: la ciberseguridad. La empresa Anthropic anunció el lanzamiento de Project Glasswing, una iniciativa que reúne a gigantes tecnológicos como Apple, Google, Microsoft y Amazon Web Services con un objetivo común: evitar que la propia IA se convierta en una amenaza difícil de controlar.

MENOS DE LA MITAD DE LOS ORGANISMOS PÚBLICOS ESTÁN PREPARADOS ANTE UNA CRISIS TECNOLÓGICA

el destape - a continuidad operativa dejó de ser un escenario excepcional para convertirse en un desafío diario para empresas y organismos públicos. Cortes de energía en picos de demanda, tormentas intensas y sistemas exigidos al límite exponen una realidad: sin infraestructura tecnológica robusta, sostener servicios críticos sin interrupciones es cada vez más difícil. El problema es que la preparación todavía no está a la altura. Según un estudio de Splunk, solo el 42% de los organismos públicos se considera bien preparado en términos de resiliencia digital. Aún así, la tendencia global marca un cambio de rumbo: el 65,5% de las organizaciones ya aumentó su inversión en continuidad del negocio, mientras que el 45,4% cuenta con un responsable específico que reporta al directorio.

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.