DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 16, 2026

DIGI AMERICAS ALLIANCE MEMBERS

GOBIERNO ACTIVA PLAN DE CIBERSEGURIDAD TRAS ATAQUES A DIGECAM Y LABORATORIO NACIONAL - GUATEMALA

Soy 502 - El Organismo Ejecutivo informó que contempla una serie de acciones para fortalecer la protección de las instituciones públicas frente a ataques cibernéticos. Dichas acciones se darán en el marco del Plan de Transformación Digital que incluye la implementación del Sistema Nacional de Ciberseguridad, confirmó la Secretaría de Comunicación Social de la Presidencia. Estas medidas se impulsan en un contexto reciente marcado por incidentes de seguridad informática, entre ellos el ataque a la Dirección General de Control de Armas y Municiones (Digecam), en el que se vio comprometida información institucional, así como el intento de ciberataque al Laboratorio Nacional de Salud.

LEY "ANTILAVADO" Y DE CIBERSEGURIDAD ENCABEZAN AGENDA - GUATEMALA

Congreso.gob.gt - A solicitud del diputado Jorge Mario Villagrán, jefe del bloque Azul, fue incluida, también, para su tercer debate la iniciativa 6347, que impulsa una ley de ciberseguridad, con el propósito de establecer un marco jurídico integral para prevenir, investigar y sancionar los delitos cibernéticos, así como para fortalecer las capacidades institucionales de respuesta ante incidentes cibernéticos para fortalecer la seguridad de los guatemaltecos, ante las amenazas digitales.

ECA DIGITAL MUDA REGRAS DA INTERNET PARA CRIANÇAS E ADOLESCENTES: VEJA COMO FUNCIONA A PROTEÇÃO DE DADOS E O QUE FAZER PARA GARANTIR SEGURANÇA ONLINE - BRASIL

E.M. Foco - O aumento da presença de crianças e adolescentes na internet levou à criação de novas regras específicas para esse público no ambiente on-line. Com o chamado ECA Digital, o Brasil passa a detalhar como devem funcionar a proteção de dados, a moderação de conteúdo, a publicidade e a responsabilidade de empresas e responsáveis legais em relação ao uso de plataformas digitais por menores, aproximando o mundo virtual das garantias já previstas no Estatuto da Criança e do Adolescente.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 16, 2026

QUANDO O RISCO CIBERNÉTICO NASCE NA SALA DE REUNIÕES - BRASIL

Defesa Net - A maior ameaça à segurança digital das empresas não vem de hackers sofisticados: vem das decisões estratégicas tomadas por CEOs, CFOs e CTOs que, sem perceber, abrem portas para ataques tão devastadores quanto qualquer invasão externa. De acordo com dados de mercado, violações de dados envolvendo terceiros dobraram no ano passado. Ao menos 82% das brechas afetam dados armazenados em nuvem, e mais de 60% dos aplicativos corporativos operam como “shadow IT” – fora do controle das equipes de segurança. No Brasil, onde apenas 5% das organizações atingem maturidade em cibersegurança, o custo médio de um vazamento já alcança R$ 7,19 milhões.

PARTICIPA SSPE EN CAPACITACIÓN INTERNACIONAL SOBRE CIBERSEGURIDAD - MÉXICO

El Diario de Chihuahua - Un elemento de la Secretaría de Seguridad Pública del Estado (SSPE), encabezada por el secretario Gilberto Loya, participó en un programa internacional de líderes en materia de ciberseguridad, desarrollado en Estados Unidos, con el objetivo de fortalecer las capacidades tecnológicas y estratégicas en la prevención y combate del cibercrimen. En representación de México, acudió Daniel Aranda Viezcas, adscrito a la Subsecretaría de Inteligencia y Análisis Policial, quien formó parte de este encuentro junto a delegaciones de países como Brasil, Guatemala, Argentina, Paraguay, Uruguay y Chile.

ARGENTINA ACELERA UN ACUERDO DE CIBERSEGURIDAD CON ESTADOS UNIDOS: ALCANCE, CONTEXTO Y QUÉ CAMBIA

IT.Sitio - El Gobierno de Argentina, liderado por Javier Milei, avanza en la negociación de un acuerdo de ciberseguridad con Estados Unidos con un objetivo concreto: fortalecer la capacidad del Estado para prevenir y responder a ataques informáticos en un escenario donde reconoce limitaciones estructurales. El Ejecutivo busca acceder a financiamiento, cooperación técnica y equipamiento para reforzar los sistemas de protección estatal, en un contexto en el que admite vulnerabilidades en distintas áreas de la administración pública. La iniciativa no aparece como un hecho aislado. Forma parte de una estrategia más amplia de alineamiento con Washington en materia de seguridad, defensa e inteligencia, que redefine el posicionamiento internacional de la Argentina.

ANTHROPIC Y OPENAI ENDURECEN CONTROLES ANTE RIESGOS CRECIENTES DE IA EN CIBERSEGURIDAD

Diario Bitcoin - Las principales compañías de inteligencia artificial, Anthropic y OpenAI, han comenzado a implementar medidas más estrictas para controlar el acceso a sus tecnologías, en respuesta al creciente riesgo que representan sus modelos en el ámbito de la ciberseguridad. Lo que inicialmente surgió como herramientas orientadas a tareas cotidianas ha evolucionado rápidamente hacia sistemas capaces de identificar y explotar vulnerabilidades críticas, elevando las preocupaciones a nivel de seguridad nacional.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 16, 2026

FBI: RANSOMWARE STILL A TOP THREAT TO CRITICAL INFRASTRUCTURE - USA

Gov Tech - Ransomware continues to pose a serious threat to U.S. critical infrastructure, with more than 2,100 related incidents reported to federal authorities in 2025, according to the latest FBI Internet Crime Complaint Center (IC3) report. To put that number in perspective, IC3 reported roughly 1,100 data breach threats to critical infrastructure, which includes sectors such as health care, critical manufacturing, financial services, energy and agriculture, among others. Ransomware attacks directed at critical infrastructure are serious, possessing as they do the potential to disrupt operations, expose sensitive data and affect the delivery of public services.

CYBERATTACKS TARGET US INFRASTRUCTURE, AND OTHER CYBERSECURITY NEWS

WEF - A new joint advisory from US agencies has said that cyber activity targeting critical infrastructure has escalated in recent weeks amid the conflict in the Middle East, highlighting how geopolitical tensions are increasingly playing out in cyberspace. Hackers are exploiting internet-exposed operational technology (OT) devices — which are connected to the internet for remote monitoring, exposing infrastructure to attacks — used across sectors including energy, water and local government systems. The advisory notes that the widespread use of these devices and their frequent exposure to the public internet make them an attractive target for hackers. In several cases, these events have already caused operational disruption and financial loss, with attackers manipulating data on industrial control interfaces and extracting sensitive system files.

BRUTE-FORCE CYBERATTACKS ORIGINATING IN MIDDLE EAST SURGE IN Q1

Cybersecurity Dive - A surge of brute force authentication attacks targeted network devices during the first quarter of 2026, with the vast majority of threat activity coming from the Middle East. Almost 90% of the brute-force attacks originated from various Middle East locations, and the leading targets were SonicWall and Fortinet FortiGate devices. IP addresses alone are not considered a reliable indicator, but said it was “safe to assume” that a combination of state-linked and professional groups were involved. Attacks from opportunistic groups were also likely involved. Hackers have been aggressively scanning perimeter devices for weak or exposed credentials, according to the blog post.

OAS AND MASTERCARD JOIN FORCES TO COMBAT CYBERCRIME

OAS - The Organization of American States (OAS) and the company Mastercard signed an agreement today to work together to strengthen cyber resilience in the Americas, during a ceremony held at the headquarters of the hemispheric institution in Washington, DC. The OAS Secretary for Multidimensional Security, Ivan Marques, highlighted how cybercrime, ransomware, and attacks on critical infrastructure are growing in scale and sophistication, affecting governments, businesses, and citizens alike. “Addressing these challenges requires more than government action alone. The private sector is at the forefront of innovation and expertise in cybersecurity. Companies like Mastercard are essential partners in securing financial systems and building trust in digital commerce,” added Secretary Marques, who signed the Memorandum of Understanding on behalf of the OAS Secretary General, Albert R. Ramdin.