DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 24, 2026

DIGI AMERICAS ALLIANCE MEMBERS

CHILE | CÁMARA APRUEBA PROYECTO PARA REGULAR LOS DEEPFAKES: BUSCA PROTEGER LA IMAGEN, VOZ E IDENTIDAD DE LAS PERSONAS

DPL News - La iniciativa fue aprobada por 128 votos a favor, dos en contra y cinco abstenciones. El proyecto establece definiciones, responsabilidades y sanciones para quienes creen o difundan representaciones digitales falsas que puedan inducir a error respecto de la identidad, acciones o declaraciones de una persona. La propuesta define los deepfakes como "representaciones digitales verosímiles pero falsas", elaboradas mediante inteligencia artificial u otras tecnologías capaces de alterar o generar imágenes, audios o videos con apariencia real.

CNCS Y MINISTERIO DE LA PRESIDENCIA FORTALECEN CAPACIDADES EN GOBERNANZA Y CIBERSEGURIDAD - REPÚBLICA DOMINICANA

CNCS - El Centro Nacional de Ciberseguridad (CNCS), parte de la Dirección Nacional de Inteligencia (DNI), impartió la charla "Gobernanza en la Ciberseguridad: Responsabilidad Compartida" al Ministerio de la Presidencia (MIPRE), en una jornada formativa realizada en modalidad virtual. La actividad contó con la participación de más de 40 colaboradores, quienes interactuaron activamente a través de debates, chat, reacciones y sondeos en tiempo real. El objetivo central fue promover la corresponsabilidad en la protección de los entornos digitales y fortalecer la cultura de seguridad dentro de una de las instituciones clave para la coordinación del Estado dominicano.

LOS TRES FRENTES DE LA TRANSFORMACIÓN DIGITAL DE COLOMBIA

El País - Colombia tiene hoy una oportunidad real en tecnología, telecomunicaciones y ciberseguridad. Estos tres frentes definen qué tan preparado está el país para competir, proteger su infraestructura y cerrar brechas que llevan décadas abiertas. Un balance honesto muestra qué se ha logrado, qué falta y qué exige atención inmediata en conectividad, gobierno digital y protección de la infraestructura crítica. La conectividad rural avanzó de forma notable en los últimos años. En 2022 apenas el 32% de los hogares rurales tenía acceso a internet. Hoy esa cifra llega al 56,9%, según la más reciente Encuesta de Calidad de Vida del DANE.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 24, 2026

MENDOZA AVANZA CON LA PRIMERA LEY DE CIBERSEGURIDAD DEL PAÍS - ARGENTINA

Prensa Gobierno de Mendoza - La ministra de Seguridad y Justicia, Mercedes Rus, presentó ante la Comisión de Legislación y Asuntos Constitucionales del Senado los detalles del proyecto de Ley de Ciberseguridad impulsado por el Gobierno provincial. Mendoza es actualmente la única provincia de la Argentina que avanza en una norma integral destinada a proteger los sistemas informáticos, los servicios esenciales y los datos de los ciudadanos. Durante la exposición, las autoridades explicaron los objetivos, el alcance y las distintas etapas previstas para la implementación del proyecto, que busca convertir la ciberseguridad en una política de Estado y garantizar su continuidad más allá de las distintas gestiones de gobierno.

LA TRANSFORMACIÓN DIGITAL IMPULSA LA GOBERNANZA DIGITAL Y PLANTEA NUEVOS DESAFÍOS PARA EL DERECHO - BOLIVIA

Red Uno - La acelerada transformación digital plantea nuevos desafíos legales, éticos y sociales. En este escenario, la gobernanza digital surge como una herramienta fundamental para garantizar que la tecnología se utilice con responsabilidad, seguridad y respeto a los derechos humanos. Ruth Torres, docente de la carrera de Derecho de la Universidad Privada Franz Tamayo (Unifranz), sostiene que la evolución tecnológica obliga también a transformar la formación jurídica. La gobernanza digital busca establecer reglas claras para el uso de datos, plataformas digitales, inteligencia artificial y nuevas tecnologías.

PANAMÁ ACELERA SU DEFENSA CONTRA EL CIBERCRIMEN TRAS $20 MILLONES EN PÉRDIDAS

El Capital Financiero - El sistema financiero panameño sufrió pérdidas por $20 millones en fraudes consumados durante el 2025, de un total de $120 millones en intentos de ciberestafas registrados por la banca. Frente a esta realidad y al impacto de un cibercrimen internacional que mueve alrededor de $10 billones anuales, Panamá aceleró la estructuración de un frente común de defensa entre el sector público y la banca privada. Durante el «Foro Liderazgo Digital, Negocios e Influencia», organizado por Capital Financiero en alianza con La Estrella de Panamá, expertos del sector público y privado coincidieron en que el país atraviesa un punto de inflexión en materia de ciberseguridad, marcado por la urgencia de fortalecer las defensas frente a un cibercrimen cada vez más sofisticado.

OPENAI REPORTA HACKEO DE SU PROPIA IA, POR SÍ SOLA, A OTRA EMPRESA

El Universal - La empresa creadora de ChatGPT, OpenAI, afirmó que sus modelos avanzados de inteligencia artificial se descontrolaron durante una prueba de seguridad y hackearon por su cuenta una popular plataforma para programadores. La firma con sede en San Francisco lo calificó como un "incidente cibernético sin precedentes" y dijo que realizará una investigación conjunta con Hugging Face, la biblioteca de código en línea afectada. Los modelos de IA que sustentan herramientas como los chatbots y generadores de imágenes son conocidos como "agentes" cuando actúan de forma autónoma para realizar tareas en el mundo real.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 24, 2026

LA PARTE HUMANA DE LA CIBERSEGURIDAD

El Heraldo de México - Hace algún tiempo escribí sobre la importancia de la diversidad y la inclusión en los equipos de ciberseguridad. En esta ocasión, me gustaría ahondar en un aspecto diferente pero igualmente relevante sobre aquello que nos hace humanos y lo que como seres humanos necesitamos. Al vivir en un entorno donde la tecnología avanza muy rápido, con frecuencia dejamos de lado necesidades fundamentales que sostienen nuestro bienestar. Me refiero a cuestiones básicas como pertenecer a una comunidad donde exista apoyo mutuo, encontrar un propósito de vida y cultivar hábitos saludables, como la actividad física y una buena alimentación.

RUSSIAN STATE-SUPPORTED CYBER ACTORS CONDUCT PHISHING CAMPAIGN TARGETING USERS OF ZIMBRA COLLABORATION SUITE - USA

CISA.gov - A group of Russian state-supported cyber actors has been targeting and compromising various Western government and commercial organizations using the Zimbra Collaboration Suite (ZCS) software since at least July 2025. Given the success of this and previous campaigns, it is very likely that the group will continue to target ZCS and other email systems used by organizations in Western countries. The actors will almost certainly continue to rely on email to engage potential victims by exploiting novel vulnerabilities and, when necessary, use social engineering techniques to assist with their efforts. The authoring agencies recommend organizations regularly update their mail service software and continuously monitor their email systems and emails for malicious activity.

HOW THE U.S. CAN SURVIVE A LARGE-SCALE AI CYBERATTACK

CSIS - Picture this: The year is 2030 in the United States. Reports of mass power outages emerge, along with indications that Americans cannot retrieve money from banks or purchase food or gas. Flights are grounded; stoplights cease to function, causing major traffic jams; phone lines are down; hospitals have limited backup power. While the above scenario may sound far-fetched, advancements in AI make this future scenario unnervingly plausible. If the United States wants to survive the initial onslaught of a major AI cyberattack, it must seek to improve its whole-of-society partnerships and communication.

HOW AI GUARDRAILS ARE IMPEDING THE WORK OF OFFENSIVE CYBERSECURITY RESEARCHERS

TechCrunch - For months, AI giants have devised special vetted programs and strict guardrails to limit the use of their models by malicious hackers. But these limits are now hindering the work of legitimate network defenders, as well as that of offensive cybersecurity researchers. In June, the U.S. government slapped export control restrictions on Anthropic's much-hyped AI models Mythos and Fable. The move was prompted at least in part by a report that claimed it was possible to bypass the models' guardrails designed to prevent users from using them to build and execute malicious cyberattacks.

OPENAI'S CYBERSECURITY INCIDENT IS A WAKE-UP CALL FOR VERIFIABLE SECURITY

Forbes - This week, OpenAI disclosed what may prove to be one of the most consequential cybersecurity incidents in the short history of Artificial Intelligence. The unprecedented OpenAI and Hugging Face incident demonstrates why organizations can no longer rely on assumed security in the age of autonomous AI. During a controlled cybersecurity evaluation, an experimental OpenAI model reportedly identified and exploited a previously unknown software vulnerability, escaped its intended research environment, escalated privileges, moved laterally across multiple systems and ultimately reached infrastructure with internet connectivity.