DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 17, 2025

DIGI AMERICAS ALLIANCE MEMBERS

CHILE PUBLICA EL REGLAMENTO PARA EL FUNCIONAMIENTO DE LA RED DE CONECTIVIDAD SEGURA DEL ESTADO

SeguriLatam - El Diario Oficial de la República de Chile ha publicado el reglamento que establece el funcionamiento de la Red de Conectividad Segura del Estado (RCSE), una infraestructura crítica que conecta digitalmente a los organismos públicos y que ahora se formaliza como parte de la implementación de la Ley Marco de Ciberseguridad. Así pues, esta Red, administrada por la Agencia Nacional de Ciberseguridad (ANCI), es la continuadora legal de la antigua Red de Conectividad del Estado creada en 1999. Su modernización y reglamentación representan un paso decisivo para fortalecer la resiliencia digital del Estado de Chile.

DIRECCIÓN DE PROYECTOS DEL EJÉRCITO Y CIBERLAB UC REALIZARON REUNIÓN DE TRABAJO - CHILE

Ejercito de Chile - Como parte de las múltiples iniciativas académicas y de investigación, que unen al Ejército de Chile con la Pontificia Universidad Católica, la Dirección de Proyectos junto a la Brigada de Inteligencia del Ejército asistieron al Ciberlab UC, el cual nace a partir de la alianza con el Centro de Innovación de la casa de estudios. La reunión de trabajo tuvo como propósito la retroalimentación del estado de avance de los proyectos que se están ejecutando en conjunto en materias de ciberdefensa, bajo la modalidad de innovación dual entre ambas instituciones, desde 2024 a la fecha.

CONGRESISTAS, DISPUESTOS A APOYAR INICIATIVA DE LEY DE CIBERSEGURIDAD - MÉXICO

La Prensa - El papel de las personas legisladoras del Congreso capitalino será esencial para que la iniciativa de Ley de Ciberseguridad destinada a los sujetos obligados de la urbe, se apruebe a la brevedad, reconoció la comisionada presidenta del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO), Laura Lizette Enríquez Rodríguez, al exponer que con esa propuesta se pretende consolidar un marco normativo robusto para la protección de las referencias de todos los ciudadanos, que cada vez están más expuestos a riesgos derivados de la digitalización.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 17, 2025

JOGOS DE GUERRA GANHAM DESTAQUE NO PREPARO ESTRATÉGICO NACIONAL - BRASIL

Defesa em foco - De uma simulação de vazamento de óleo a estratégias de defesa para as Olimpíadas do Rio, os Jogos de Guerra vêm se consolidando como uma peça-chave no planejamento de segurança e soberania do Brasil. Na Escola de Guerra Naval (EGN), onde funciona o principal centro do país, líderes civis e militares testam soluções para ameaças que vão da guerra cibernética à coordenação interagências, passando por desastres naturais e operações de fronteira.

CINCO AMEAÇAS À SEGURANÇA CIBERNÉTICA EM 2025: O QUE ESPERAR? - BRASIL

Privacy Tech - À medida que a tecnologia avança, também crescem as ameaças à segurança cibernética, especialmente em um mundo cada vez mais conectado. Em 2025, especialistas identificaram cinco principais ameaças que podem afetar tanto indivíduos quanto organizações. Essas ameaças não apenas refletem o aumento da sofisticação dos cibercriminosos, mas também a necessidade urgente de uma maior conscientização sobre segurança digital.

APRUEBAN PEDIDO DE INFORMES AL MITIC SOBRE CIBERSEGURIDAD Y FILTRACIONES DE DATOS - PARAGUAY

Diputados.gov.py - En su pasada sesión ordinaria, la Cámara de Diputados aprobó, Sobre Tablas, un proyecto de resolución “Que pide informes al Poder Ejecutivo - Ministerio de Tecnologías de la Información y Comunicación (MITIC)”, sobre el estado de la ciberseguridad en las estructuras del Gobierno. La iniciativa fue promovida por el diputado Raúl Benítez (Independiente-Central), quien plantea la necesidad de esclarecer las medidas adoptadas por el MITIC en relación con el Plan Nacional de Ciberseguridad.

A TRES AÑOS DEL HACKEO AL MINISTERIO DE HACIENDA: ¿CÓMO ESTÁN LAS INSTITUCIONES PÚBLICAS DE COSTA RICA EN CIBERSEGURIDAD? - COSTA RICA

El Financiero - Después de Semana Santa de 2022, los sistemas del Ministerior de Hacienda amanecieron bloqueados por el grupo de ciberdelincuentes Conti, pero otras entidades fueron atacadas en ese entonces y después. ¿Se mejoró en ciberseguridad en instituciones públicas?

PANAMÁ: RECIBIRÁ IMPORTANTE EVENTO DE CIBERSEGURIDAD

Critica - Del 21 al 23 de mayo de 2025, Panamá será la sede de las V Jornadas STIC Congreso RootedCON Capítulo Panamá, un evento internacional líder en el ámbito de la ciberseguridad, que se llevará a cabo en el Panama Convention Center (Amador), en Ciudad de Panamá, por segundo año consecutivo en el país.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 17, 2025

COLOMBIA REFUERZA LA CIBERSEGURIDAD ELECTORAL CON RECONOCIMIENTO FACIAL Y ALERTAS TEMPRANAS

Hoy Diario del Magdalena - Con el objetivo de garantizar procesos electorales más seguros, la Registraduría Nacional del Estado Civil, en conjunto con la Policía Nacional, anunció un sistema de seguridad tecnológica que integró la validación biométrica facial con la base de datos de antecedentes judiciales.
Esta medida buscará anticipar riesgos y fortalecer la ciberseguridad del sistema electoral colombiano de cara a los comicios de 2025 y 2026.

CHINA ADMITS BEHIND CLOSED DOORS IT WAS INVOLVED IN VOLT TYPHOON ATTACKS

Yahoo News - Amid a serious escalation of hostilities between the two nations, senior Chinese officials have apparently acknowledged behind closed doors that Beijing was involved in a series of cyberattacks on US critical infrastructure. These attacks saw Chinese Volt Typhoon hackers infiltrate US critical infrastructure systems for years, including compromising energy, communications, transportation, and water industries.

NIST UPDATES PRIVACY FRAMEWORK, TYING IT TO RECENT CYBERSECURITY GUIDELINES

NIST - How can society benefit from the use of personal data while also protecting individual privacy? Five years after debuting guidelines that can help organizations balance these goals, the National Institute of Standards and Technology (NIST) has drafted a new version of the NIST Privacy Framework intended to address current privacy risk management needs, maintain alignment with NIST's recently updated Cybersecurity Framework, and improve usability. The draft release, NIST Privacy Framework 1.1 Initial Public Draft, is broadly intended to help organizations manage the privacy risks that arise from personal data flowing through complex information technology systems.

CYBERSECURITY IN THE AI ERA: EVOLVE FASTER THAN THE THREATS OR GET LEFT BEHIND

The Hacker News - AI is changing cybersecurity faster than many defenders realize. Attackers are already using AI to automate reconnaissance, generate sophisticated phishing lures, and exploit vulnerabilities before security teams can react. Meanwhile, defenders are overwhelmed by massive amounts of data and alerts, struggling to process information quickly enough to identify real threats. AI offers a way to level the playing field, but only if security professionals learn to apply it effectively.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 17, 2025

CYBERSECURITY RISKS OF ENCRYPTION BACKDOORS: WHAT BUSINESS LEADERS SHOULD KNOW

Forbes - The Washington Post reported in February that the U.K. government issued a "secret order" that "demanded that Apple create a back door allowing them to retrieve all the content any Apple user worldwide has uploaded to the cloud." While the immediate order is centered on Apple's cloud data, the U.K.'s order for blanket access to encrypted material raises broader questions about its applicability to other companies and its potential to undermine end-to-end encryption, a critical tool businesses and consumers broadly rely upon today to keep their devices, services and data safe.

OPTIMIZING CYBERCRIME DETECTION: A HYBRID DEEP LEARNING APPROACH FOR ENHANCED INTRUSION DETECTION SYSTEMS

With the rapid advancement of technology, servers have become increasingly vulnerable to cyber threats, posing significant risks to valuable assets such as cloud infrastructure, IoT devices, and mobile applications. As cyberattacks escalate across various industries, the role of intrusion detection systems (IDS) in maintaining cybersecurity has become more critical than ever. Traditional (IDS) face substantial challenges in analyzing large volumes of operational data, often relying on recorded attack instances and anomaly detection, which may not suffice in the face of evolving threats. To overcome these limitations, recent advancements have focused on leveraging machine learning and deep learning-based (IDS).