DIGI AMERICAS ALLIANCE MEMBERS

COMIENZA A OPERAR LA AGENCIA NACIONAL DE CIBERSEGURIDAD (ANCI) Y PRESIDENTE DESIGNA A DANIEL ÁLVAREZ COMO SU PRIMER DIRECTOR - CHILE

Trendtic - En el proceso de implementación de la Ley 21.663 Marco de Ciberseguridad, aprobada por unanimidad por el Congreso en diciembre de 2023, el jueves 2 de enero comenzó a operar la Agencia Nacional de Ciberseguridad (ANCI). La Ley Marco, incluida la creación de la ANCI, es parte de la agenda priorizada de seguridad del gobierno. El nuevo organismo se enmarca en la Estrategia de Seguridad del Gobierno, en los ejes de fortalecimiento de las instituciones, combate al crimen organizado -particularmente para enfrentar los ciberdelitos- y también en la búsqueda de acuerdos de Estado en materia de seguridad. Entre las facultades de la ANCI está fiscalizar, regular y sancionar a instituciones prestadoras de servicios esenciales, sean públicas o privadas en materia de ciberseguridad.

LEY MARCO DE CIBERSEGURIDAD EN CHILE OBLIGA A LAS EMPRESAS A FORTALECER SU PROTECCIÓN DIGITAL: GUÍA PARA ALINEARSE A LA NORMA

Emol - En respuesta al creciente panorama de amenazas cibernéticas, la reciente Ley Marco de Ciberseguridad en Chile exige que las organizaciones adopten medidas urgentes para proteger sus sistemas y datos críticos. La normativa busca no solo reforzar la seguridad digital del país, sino también asegurar que las empresas estén preparadas para responder eficazmente a posibles ataques. Carolina Pizarro, Cybersecurity Associate Director de Accenture Chile, destacó que la norma obliga a las empresas a implementar una serie de prácticas clave para fortalecer su ciberseguridad: “Esto incluye no solo la capacidad de responder rápidamente a los incidentes, sino también la de recuperarse de ellos de manera efectiva, minimizando el impacto en los servicios y en la población”.

COMISSÃO DE RELAÇÕES EXTERIORES AVALIA POLÍTICA NACIONAL DE CIBERSEGURANÇA - BRASIL

Senado - O Relatório de avaliação do senador Esperidião Amin (PP-SC) aponta prioridades para setor que levanta preocupações devido a crescentes ataques cibernéticos. Crítica à criação da Política Nacional de Cibersegurança (decreto nº 11.856/2023) pelo governo e necessidade de uma agência são destaques no texto do relator.

PREOCUPACIÓN ENTRE PERIODISTAS POR NUEVA LEY DE CIBERSEGURIDAD EN EL SALVADOR

CNN - La Asamblea Legislativa de El Salvador aprobó las leyes de ciberseguridad y de protección de datos personales. Según algunas organizaciones locales, y otras internacionales como Human Rights Watch, estas normas podrían limitar las libertades de expresión y de acceso a la información. Por su parte, el Gobierno rechaza las críticas.

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN - ECUADOR

El Comercio - El EGSI v3 en Ecuador refuerza la ciberseguridad pública, protegiendo datos sensibles mediante gestión de riesgos, controles técnicos y cumplimiento normativo, garantizando la seguridad digital como derecho clave.

FISCALÍA DESMANTELA RED DE CIBERDELINCUENTES QUE SUPLANTABA ENTIDADES PÚBLICAS PARA COMETER FRAUDES - COLOMBIA

Caracol - La Fiscalía con ayuda de la Policía Nacional, logró identificar y capturar a tres presuntos integrantes de una red de ciberdelincuentes dedicada a suplantar entidades públicas para distribuir correos electrónicos maliciosos. Estos mensajes contenían software diseñado para extraer información personal y financiera de los dispositivos de las personas victimas facilitandoles la comisión de hurtos y otros fraudes.

LA CRISIS DEL SILENCIO DIGITAL EN ARGENTINA: LOS PELIGROS DE OCULTAR UN CIBERATAQUE - ARGENTINA

Clarin - "Dani, ¿cómo estás? Imagino que estás más que al tanto del tema del Churruca y el ciberataque de ransomware". Un jueves cualquiera se transformó en el día que la crisis de ciberseguridad que vengo señalando durante años se materializó en la voz de un amigo: "Mis viejos perdieron toda la historia clínica y estudios que les realizaron. Sobre todo mi mamá, que está en tratamiento activo... Se perdieron todos los turnos". Una “locura”, como él mismo lo definió, que desnuda la verdadera dimensión humana de nuestra indefensión digital.

ALERTA LA SSPC SOBRE INCREMENTO DE FRAUDES EN LÍNEA - MÉXICO

La Jornada - La Dirección General de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico, de la Secretaría de Seguridad y Protección Ciudadana (SSPC), alertó a la ciudadanía sobre el incremento de fraudes en línea y emitió recomendaciones para evitar ser víctimas de ciberdelincuentes. Indicó que la facilidad para realizar compras por medio de diversas plataformas, ya sea con un dispositivo móvil o una computadora, también ha incrementado que los ciberdelincuentes utilicen señuelos como son mensajes, llamadas y extraordinarias ofertas para robar datos de los usuarios y cometer estafas, por lo que, indicó, es muy importante tomar precauciones.

CAVAPY REAFIRMA SU COMPROMISO CON EL MERCADO AL GARANTIZAR SEGURIDAD INTERNACIONAL Y LA PROTECCIÓN DE LOS ACTIVOS - PARAGUAY

Marketdata - La Caja de Valores del Paraguay (Cavapy) inició un ambicioso programa de ciberseguridad que no solo busca alinearse con las exigencias locales de la Superintendencia de Valores y el Banco Central del Paraguay, sino también posicionarse como un referente regional, adoptando certificaciones internacionales como la ISO 27001 en su versión más reciente de 2022.

BIDEN ADMINISTRATION PROPOSES NEW CYBERSECURITY RULES TO LIMIT IMPACT OF HEALTHCARE DATA LEAKS

Reuters - Healthcare organizations may be required to bolster their cybersecurity, to better prevent sensitive information from being leaked by cyberattacks like the ones that hit Ascension and UnitedHealth (UNH.N), opens new tab, a senior White House official said Friday. Anne Neuberger, the U.S. deputy national security advisor for cyber and emerging technology, told reporters that proposed requirements are necessary in light of the massive number of Americans whose data has been affected by large breaches of healthcare information.

WHITE HOUSE LAUNCHES CYBERSECURITY LABEL PROGRAM FOR CONSUMERS

Cyberscoop - The White House announced Tuesday the official launch of the U.S. Cyber Trust Mark, a cybersecurity labeling initiative aimed at enhancing the security of internet-connected devices.
The initiative tackles rising consumer concerns about the security vulnerabilities of “smart” devices essential to modern homes. As households become more dependent on interconnected gadgets — with a 2023 Deloitte study revealing that the average U.S. household has 21 connected devices — the threat of cyberattacks becomes increasingly significant.

UN GENERAL ASSEMBLY ADOPTS MILESTONE CYBERCRIME TREATY

Global Issues - The General Assembly on Tuesday adopted the United Nations Convention against Cybercrime, a landmark global treaty aimed at strengthening international cooperation to combat cybercrime and protecting societies from digital threats. The agreement on the legally binding treaty marked the culmination of a five-year effort by UN Member States, with inputs from civil society, information security experts, academia and the private sector.

WHY COLLABORATION IS KEY TO DISRUPTING THE ECONOMICS OF CYBERCRIME

WEF - Businesses worldwide are embracing digital evolution. Yet cybersecurity implications inevitably emerge as technologies evolve and push us into a new era of connectivity. Adopting new technologies, devices and platforms increases potential points of compromise, widening an organization's attack surface. Having more digital systems to configure, integrate and manage leads to greater complexity and an increased likelihood of error.

THE TRUST IMPERATIVE: 5 LEVERS FOR SCALING AI RESPONSIBLY

WEF - At a recent conference, in a room with over 100 Fortune 500 founders, only two had mission-critical generative artificial intelligence (GenAI) use cases in production. The reason? Quality, accuracy and hallucinations are holding them back. This lack of trust in centring AI in their business was echoed in a recent Edelman study, which found that trust in AI companies in the United States has fallen from 50% to 35% over the last five years.

WHY SYSTEMIC INTERVENTION IS KEY TO MITIGATING CYBERCRIME

WEF - From the infrastructure that powers our villages and cities and the way we do business, to the ways we communicate with each other and entertain ourselves, we all rely on the internet. But the rise in internet use has been accompanied by an equivalent rise in attacks and cybercrime. Internet disruptions can be anything from annoying, to costly, to catastrophic. A massive data breach of background check company National Public Data in April 2024 leaked 2.9 billion US social security records, with class action lawsuits following.