

DIGI AMERICAS ALLIANCE MEMBERS



VAZAMENTO DE DADOS BANCÁRIOS AUMENTA PREOCUPAÇÃO COM FRAUDES E GOLPES NO BRASIL

AJN - O vazamento de dados bancários é uma crescente preocupação entre os brasileiros, especialmente com o aumento de fraudes e golpes. Apesar da Lei Geral de Proteção de Dados (LGPD) ter sido implementada em 2020, ainda não existe uma legislação específica que trate dos danos causados por esses incidentes, dificultando a obtenção de indenização pelas vítimas. Conforme explica a advogada e professora de Direito da Universidade Tiradentes (Unit), Clara Machado, a LGPD não diferencia tipos de dados vazados. "Quando ocorre um vazamento, a empresa ou instituição financeira pode ser multada, com penalidades variando de 2% a 10% do faturamento, limitadas a 50 milhões de reais, conforme estipulado pela LGPD", esclarece.

ATIVADO O CENTRO DE DEFESA CIBERNÉTICA DA AERONÁUTICA - BRASIL

Defesa Aerea & Naval - Na manhã desta quinta-feira (11/07), ocorreu nas dependências do Comando da Aeronáutica (COMAER), em Brasília (DF), a cerimônia militar para ativar a estrutura do Centro de Defesa Cibernética da Aeronáutica (CDCAER), sendo designado o Coronel Silvio Roberto Assunção de Oliveira Filho para ser o primeiro Chefe. O evento marca um avanço significativo na estratégia de segurança cibernética do COMAER. O CDCAER foi criado para gerenciar, executar e controlar todas as atividades relacionadas à defesa cibernética no âmbito da Aeronáutica. Subordinado diretamente à Diretoria de Tecnologia da Informação da Aeronáutica (DTI), o Centro faz parte do Sistema Militar de Defesa Cibernética, cujo órgão central é o Comando de Defesa Cibernética.

RESOLUCIÓN SOBRE DECRETO DE CIBERSEGURIDAD 5G ESTÁ EN FASE DE NOTIFICACIÓN

CRHoy - La resolución sobre el proceso relacionado con el reglamento de ciberseguridad para redes 5G está en fase de notificación. "Se consultó al TACA e indican que en ese expediente la resolución se encuentra en fase de notificación a las partes", informó la oficina de Prensa del Poder Judicial tras consulta de este medio. El caso se refiere al expediente 24-001014-1027-CA-4, que se tramita en el Tribunal Contencioso Administrativo (TCA). El mismo tiene que ver con la medida cautelar que deja sin efecto temporal los alcances del Decreto Ejecutivo 44196-MSP-MICIIT.

BLINKEN ANUNCIA CUMBRE DE LÍDERES EN COSTA RICA QUE ABORDARÍA TEMA DE SEMICONDUCTORES

CRHoy - El secretario de estado de EE UU, Antony J. Blinken, anunció este miércoles que el año entrante se realizará una cumbre de líderes en Costa Rica en la que se abordaría el tema de la industria local de semiconductores. El anuncio lo hizo en la sesión ministerial de los países de la Alianza para la Prosperidad Económica en las Américas (APEP) que entre otras cosas busca crear oportunidades para que los miembros exploren formas colaborativas para fortalecer la cadena de suministro de microchips, mediante el desarrollo de la capacidad de mano de obra calificada. Acerca de los posibles asuntos por tratar en la actividad, la Embajada de Estados Unidos indicó que "todavía es muy pronto para tener establecida la agenda para la cumbre del 2025, pero los anuncios de Washington D.C. explican las prioridades generales de APEP"

MILEI NOMBRA A UN EXPERTO EN BITCOIN COMO DIRECTOR DE CIBERSEGURIDAD - ARGENTINA

Criptotendencias - En un movimiento audaz, el presidente argentino Javier Milei ha designado a Ariel Waissbein, un reconocido experto en tecnología de Bitcoin, como el nuevo director de la Agencia Federal de Ciberseguridad (AFC). Este nombramiento subraya la intención del gobierno de Milei de reforzar la protección de la infraestructura informática crítica del país mediante la incorporación de conocimientos avanzados en criptografía y seguridad informática. Ariel Waissbein no es un nombre desconocido en el mundo de la seguridad informática y la criptografía. Con más de 20 años de experiencia en ciberseguridad y una sólida formación en matemáticas, Waissbein ha trabajado como consultor para empresas prominentes como CoinFabrik y BitTrap, que se especializan en el entorno de las finanzas descentralizadas (DeFi).

CIBERSEGURIDAD: LOS ACTUALES DESAFÍOS EN LA PROTECCIÓN DE DATOS - CHILE

La Tercera - Con miles de millones de ciberataques al año, Chile enfrenta una constante amenaza en el mundo digital. La implementación de políticas de ciberseguridad, el impulso de la Ley Marco y la creación de la ANCI son pasos importantes, pero la falta de profesionales capacitados y la necesidad de mejorar la infraestructura son retos críticos. En el reciente evento AWS re:Inforce 2024 en Filadelfia, se destacó la importancia de fomentar una cultura transversal de la prevención digital y la colaboración público-privada como clave para fortalecer la ciberseguridad.

CERTAL CAPACITARÁ A JUECES SOBRE CIBERSEGURIDAD TRAS CONVENIO - PARAGUAY

Judiciales - La Asociación de Jueces del Paraguay AJP, en colaboración con el Centro de Estudios en Regulación y Telecomunicaciones CERTAL, firmaron un acuerdo de cooperación que incluye la formación y actualización de jueces y juezas en temas críticos como la piratería y ciberseguridad. Con este convenio se busca fortalecer la capacidad de respuesta de los magistrados en estos delitos tan complejos y actuales como los crímenes perpetrados en línea, así como los casos referentes a la vulneración de la propiedad intelectual.

POLÉMICOS HACKTIVISTAS HABRÍAN PROVOCADO CENSURA DE TELEGRAM EN EL SALVADOR

Global Voices - El presidente de El Salvador, Nayib Bukele, se ha convertido en la cara del progreso tecnológico en Centroamérica, a pesar de los implacables ciberataques contra instituciones públicas salvadoreñas que han puesto en riesgo los datos de millones de ciudadanos. En 2021, Bukele impresionó a los espectadores internacionales cuando convirtió el Bitcoin en moneda legal en El Salvador, y en 2024 anunció la inauguración de una nueva oficina de Google en el país, con la promesa de digitalizar los sectores educativos y de salud. Sin embargo, no ha habido reconocimiento público de más de una docena de filtraciones de datos contra la infraestructura pública entre abril y junio de 2024.

LA UNIÓN HACE LA FUERZA: GRUPOS DE MUJERES EN CIBERSEGURIDAD DE LATAM

Heraldo de Mexico - La ciberseguridad, un campo crucial para todas las organizaciones, enfrenta desafíos complejos y multidimensionales que requieren de diversas perspectivas y habilidades. En dicha área las mujeres han demostrado tener un enfoque único y valioso para abordar estos retos; no obstante, la brecha de género en este sector sigue siendo una realidad en América Latina, donde las mujeres representan solo una pequeña fracción de la fuerza laboral, lo que limita el potencial y la diversidad de perspectivas en este ámbito tan importante.

AN APATHY OF CYBERSECURITY CONCERNS - T&T

Newsday - FOR JUST over a month, the website of the Guyana Cricket Board has been quite visibly defaced by hackers who demanded US\$1,000 in Bitcoin. The defacement took the form of a warning and demand, stating partly, "Your company was hacked due to major security issues and your documents, contracts, work correspondence ended up in our possession, we would love to forget this incident but we cannot, so your business partners should not suffer because of your negligence to security."

CISA PUBLISHES RESILIENCE-PLANNING PLAYBOOK FOR CRITICAL INFRASTRUCTURE

StateScoop - The Cybersecurity and Infrastructure Security Agency on Wednesday published a supplemental manual to its infrastructure resilience planning framework, which provides guidance on how local governments and the private sector can work together to improve the security and resilience of the nation's critical infrastructure. The new playbook includes processes and table top exercises to help public and private sectors minimize the impact of cyberattacks on their communities, reduce the risk of disruption to critical services and keep system restoration costs low.

RANSOMWARE ATTACKS ARE HITTING ENERGY, OIL AND GAS SECTORS ESPECIALLY HARD, REPORT FINDS

StateScoop - Ransomware attacks are hitting energy and oil and gas sectors harder, costing utilities more in recovery time and funding as victims appear increasingly willing to pay ransom demands, according to a new report from the cybersecurity firm Sophos. The report looks at ransomware impacts to critical infrastructure organizations and is based on more than 200 responses from a wider survey of 5,000 cybersecurity and IT leaders taken in January and February. Sophos said that the ransomware attack rate appears to be falling globally, but researchers found that recovery times for energy, oil and natural gas, and utilities have been steadily increasing since at least 2022.

THE NEXT FRONT IN U.S.-CHINA TECH BATTLE? UNDERWATER CABLES THAT POWER THE GLOBAL INTERNET

CNBC - U.S.-Chinese tensions surrounding technology have sunk to sea lows. Subsea cables hit the headlines earlier this year after four out of 15 critical submarine cables in the Red Sea were cut amid attacks by Yemen's Iran-backed Houthi rebels on Israeli U.S., and U.K. ships. Public awareness of submarine cables has grown as a result — and these networks of cables are becoming a new source of strain in international relations, amid heating geopolitical engagements between the U.S. and China.



INSIGHTS

JULY 18, 2024

THE RISE OF SMART CONTRACTS AND STRATEGIES FOR MITIGATING CYBER AND LEGAL RISKS

WEF - Imagine a world where contracts are executed seamlessly without human intervention, reducing costs and enhancing efficiency across industries – from finance to real estate. This is the promise of smart contracts, self-executing agreements embedded in blockchain technology. However, the rapid adoption of this revolutionary technology comes with significant risks. In 2016, a coding flaw in the Decentralized Autonomous Organization (DAO) smart contract on the Ethereum platform led to a theft of \$50 million worth of ether, illustrating the potential vulnerabilities.

DIGITAL SAFETY: ARE YOU USING ONE OF THE WORLD'S MOST POPULAR PASSWORDS?

WEF - What makes a terrible online password? Something simple, short and predictable. Astonishingly, those are also the characteristics of the world's most common online password, which is 123456, according to online password management company NordPass. NordPass also calls 123456 the worst password, because as well as being used over 4.5 million times, it takes less than a second for hackers to crack – like the rest of the top 20 most popular online passwords.