



INSIGHTS

FEBRUARY 6, 2025

DIGI AMERICAS ALLIANCE MEMBERS



CIBERSEGURIDAD, PRIORIDAD PARA EL GOBIERNO FEDERAL - MEXICO

DineroEnImagen - Por primera vez, el gobierno federal contará con una Dirección General de Ciberseguridad que diseñe, desarrolle, ejecute y actualice las estrategias y un marco de gobierno para la gestión en esta materia. Por primera vez, el gobierno federal contará con una Dirección General de Ciberseguridad que diseñe, desarrolle, ejecute y actualice las estrategias y un marco de gobierno para la gestión en esta materia. Víctor Ruiz, experto en ciberseguridad, mencionó que se trata de una propuesta muy acertada y, como plan, aborda gran parte de las necesidades actuales de la ciudadanía para protegerla frente a las ciberamenazas.

SENADO ANUNCIA FORO SOBRE IA Y CIBERSEGURIDAD - REPÚBLICA DOMINICANA

elnacional - El presidente del Senado, Ricardo de los Santos, anunció que el encuentro internacional Parlamentos y Prosperidad, República Dominicana 2025 trabajará una agenda legislativa común con países de la región para abordar temas clave como ciberseguridad, salud e inteligencia artificial. Académicos, empresarios y legisladores debatirán sobre El parlamento y la agenda digital, ciberseguridad, inteligencia artificial, El parlamento, la salud y la seguridad social, El parlamento y el crecimiento económico y El parlamento y la legislación basada en el conocimiento científico.

EE.UU. COLABORARÁ CON COSTA RICA EN TEMAS DE CIBERSEGURIDAD, MIGRACIÓN Y NARCOTRÁFICO

yahoo!noticias - El presidente de Costa Rica, Rodrigo Chaves, y el secretario de Estado de Estados Unidos, Marco Rubio, confirmaron este martes que continuarán con la cooperación bilateral en temas de ciberseguridad, migración y narcotráfico. Durante la visita oficial de Rubio a San José, el secretario de Estado indicó que Costa Rica es un país "ejemplo y modelo", así como un "amigo y aliado", con el que Estados Unidos comparte temas en común como los "valores" y la "historia".

AGENCIA NACIONAL DE CIBERSEGURIDAD DE CHILE: PRIMEROS PASOS, REFERENTES Y OBJETIVOS

dplnews - A principios de año inició funciones la Agencia Nacional de Ciberseguridad de Chile (ANCI), responsable de fiscalizar, regular y sancionar a instituciones públicas o privadas que presten servicios en la materia. Además, definirá los servicios esenciales y los operadores de importancia vital y dictará protocolos, estándares e instrucciones generales para implementar la Ley Marco de Ciberseguridad.

UE FINANCIARÁ CAPACITACIÓN PARA PYMES TICAS EN CIBERSEGURIDAD

crhoy.com - El Centro de Competencia Cibernética de América Latin y el Caribe (LAC4), en cooperación con las delegaciones de la Unión Europea (UE) en Centroamérica, convocan a las pequeñas y medianas empresas (pymes) centroamericanas a participar en una capacitación para el fortalecimiento de habilidades en ciberseguridad. La actividad que se realizará del 19 al 21 de marzo en la ciudad de Antigua, Guatemala, cuenta con el apoyo de EUreCA y busca promover buenas prácticas de ciberseguridad, para ello tres empresas de Panamá, Costa Rica, Honduras, Guatemala, Belice, y El Salvador serán invitadas a un entrenamiento presencial financiado por la UE en materia de ciberseguridad.

CIBERSEGURIDAD Y NEGOCIOS: EL CISO COMO LÍDER EN LA ERA DIGITAL

LaVerdadNoticias - Durante años, el papel del Chief Information Security Officer (CISO) se limitó a la protección de sistemas y datos, operando en un segundo plano dentro de las organizaciones. Sin embargo, en la era digital, donde los ciberataques pueden costar millones y afectar la reputación de una empresa en segundos, la ciberseguridad ya no es solo un tema técnico, sino una cuestión de negocio y estrategia corporativa. Hoy, los CISOs tienen un asiento en la sala de juntas, con la oportunidad —y la responsabilidad— de convertirse en socios estratégicos del negocio.

DEEPSEEK DESDE UNA PERSPECTIVA DE CIBERSEGURIDAD

Portal Innova - Los chatbots potenciados con IA continúan masificándose, y el más reciente desarrollado en China - DeepSeek- ha generado expectación mundial y no solo a nivel de usuario, sino que también en el ámbito corporativo. Una nueva investigación de Sophos titulada “Más allá del Hype: La realidad empresarial de la IA para la ciberseguridad”, reveló que el 89% de los líderes de TI están preocupados por los fallos de la IA Generativa, y que estos afecten negativamente las estrategias de ciberseguridad de sus empresas.

GLOBAL RANSOMWARE PAYMENTS PLUNGE BY A THIRD AMID CRACKDOWN

The Guardian - Ransomware payments fell by more than a third last year to \$813m (£650m) as victims refused to pay cybercriminals and law enforcement cracked down on gangs, figures reveal.

The decline in such cyber-attacks – where access to a computer or its data is blocked and money is then demanded to release it – came despite a number of high-profile cases in 2024, with victims including NHS trusts in the UK and the US doughnut firm Krispy Kreme.

LAW ENFORCEMENT TAKES DOWN TWO LARGEST CYBERCRIME FORUMS IN THE WORLD

Europol - A Europol-supported operation, led by German authorities and involving law enforcement from eight countries, has led to the takedown of the two largest cybercrime forums in the world. The two platforms, Cracked and Nulled, had more than 10 million users in total. Both of these underground economy forums offered a quick entry point into the cybercrime scene. These sites worked as one-stop shops and were used not only for discussions on cybercrime but also as marketplaces for illegal goods and cybercrime-as-a-service, such as stolen data, malware or hacking tools. Investigators estimate that suspects earned EUR 1 million in criminal profits.

5 RISK FACTORS FROM SUPPLY CHAIN INTERDEPENDENCIES IN A COMPLEX CYBERSECURITY LANDSCAPE

WEF - According to the World Economic Forum's Global Cybersecurity Outlook 2025, the increasing reliance on complex supply chains is leading to a more uncertain and unpredictable cybersecurity landscape. Last year saw the most significant IT outage in history, highlighting the importance of safeguarding the cybersecurity ecosystem. Five key risk factors from supply chain interdependencies have been identified that contribute to an increasingly complex landscape.

'THIS HAPPENS MORE FREQUENTLY THAN PEOPLE REALIZE': ARUP CHIEF ON THE LESSONS LEARNED FROM A \$25M DEEPPFAKE CRIME

WEF - Fraudsters used an AI deepfake to steal \$25 million from UK engineering firm Arup. Here, Arup's Chief Information Officer, Rob Greig, talks about the lessons learned. Cyber resilience in the face of increasing threats is a critical objective for any organization, according to the World Economic Forum white paper Unpacking Cyber Resilience.

THE CYBERSECURITY CRISIS: COMPANIES CAN'T FILL ROLES, WORKERS SHUT OUT

Forbes - Breaking into a cybersecurity career has never been easy and today it's more competitive than ever. At the same time, there is a well-documented cybersecurity talent shortage, with an estimated 4.8 million unfilled cybersecurity jobs globally, according to the 2024 ISC2 Cybersecurity Workforce Study. The demand for skilled professionals far outpaces supply, particularly in specialized fields such as cloud security, application security and incident response. Yet, despite this gap, companies continue to outsource critical security functions overseas rather than invest in developing homegrown talent. This has major implications not only for job seekers but also for national security.

CISA ADDS FOUR KNOWN EXPLOITED VULNERABILITIES TO CATALOG

CISA - CISA has added four new vulnerabilities to its [Known Exploited Vulnerabilities Catalog](#), based on evidence of active exploitation.

- [CVE-2024-45195](#) Apache OFBiz Forced Browsing Vulnerability
- [CVE-2024-29059](#) Microsoft .NET Framework Information Disclosure Vulnerability
- [CVE-2018-9276](#) Paessler PRTG Network Monitor OS Command Injection Vulnerability
- [CVE-2018-19410](#) Paessler PRTG Network Monitor Local File Inclusion Vulnerability

These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.