DIGI AMERICAS ALLIANCE MEMBERS

GUYANA POR FORTALECER LA CIBERSEGURIDAD ANTE LA CIBERDELINCUENCIA

Prensa Latina - El gobierno de Guyana aspira hoy a consolidar su desarrollo digital, el cual deberá estar acompañado de lo más avanzado en materia de ciberseguridad para enfrentar a la ciberdelincuencia. En tal sentido, el primer ministro Mark Phillips instó a todos los sectores a ser conscientes de las amenazas en este campo, de ahí la importancia de adquirir habilidades y equiparse con las herramientas necesarias para proteger los sistemas nacionales.

PRESIDENTE ARÉVALO INAUGURA EL EJERCICIO CIBERNÉTICO DEFENSA DEL SUR 2025 - GUATAMALA

Agencia Guatemalteca de Noticias - El presidente Bernardo Arévalo participó este sábado en la inauguración del ejercicio cibernético denominado Defensa del Sur 2025. Este ejercicio forma parte del programa Centam Guardian 2025 y se integra a una serie más amplia de eventos conjuntos destinados a mejorar la interoperabilidad, coordinación operativa y resiliencia de las fuerzas aliadas frente a amenazas multidominio.

LA CANCILLERÍA DE GUATEMALA FUE HACKEADA POR UN GRUPO DE ESPIONAJE CHINO

infobae - El sistema informático del Ministerio de Relaciones Exteriores de Guatemala fue hackeado por “grupos de espionaje cibernético con sede” en China, informó este martes la Embajada de Estados Unidos en el país. “Una revisión conjunta de ciberseguridad entre Guatemala y @Southcom identificó que todo el sistema informático fue hackeado por grupos de espionaje cibernético con sede en la República Popular de China”, indicó la embajada en un mensaje en su cuenta oficial en X.

ESTADO-MAIOR DO EXÉRCITO INTEGRA A DEFESA CIBERNÉTICA AO SISTEMA ASTROS - BRASIL

Defesa Aerea & Naval - Em cumprimento à Estratégia Nacional de Defesa, que em 2008 estabeleceu três setores estratégicos para a defesa nacional: o nuclear, o espacial e o cibernético, o Ministério da Defesa (MD) atribuiu a responsabilidade pelo desenvolvimento do setor cibernético ao Exército Brasileiro, sob a coordenação da 2ª Subchefia do Estado-Maior do Exército.

CIBERSEGURANÇA NO BRASIL: COMO EMPRESAS PODEM SE PROTEGER EM UM DOS PAÍSES MAIS ATACADOS DO MUNDO

Segurança Eletrônica - O Brasil ocupa uma posição alarmante no cenário global da cibersegurança: é o segundo país que mais sofre ataques cibernéticos no mundo. A crescente digitalização dos negócios, aliada a vulnerabilidades na proteção de dados, faz com que empresas de todos os setores se tornem alvos frequentes dos criminosos virtuais. Mas como as organizações podem se proteger de ameaças cada vez mais sofisticadas?

RED ELÉCTRICA ESPAÑOLA DESCARTA UN INCIDENTE DE CIBERSEGURIDAD EN SUS INSTALACIONES

CB24 - Tras analizar el apagón acaecido el lunes, Red Eléctrica concluye que «efectivamente no ha habido ningún tipo de intrusión en los sistemas de control que pudieran haber ocasionado el incidente». El gran apagón eléctrico que afectó al territorio peninsular de España causó pérdidas económicas de 1.600 millones de euros, equivalentes al 0,1 % del producto interior bruto (PIB), según cálculos de la principal confederación empresarial del país, la CEOE.

LUPA SOBRE LA ESTRATEGIA DE TECNOLOGÍAS CUÁNTICAS DE ESPAÑA: CUÁNTO, CÓMO Y PARA QUÉ

dplnews - España lanzó su Estrategia de Tecnologías Cuánticas con dos objetivos centrales: fortalecer su ecosistema cuántico, en investigación y mercado, y preparar a la sociedad para el cambio que suponen estas tecnologías. Destinará un presupuesto de 808 millones de euros, provenientes de los Fondos Europeos de Desarrollo Regional (Feder) y el Plan de Recuperación; estiman en mil 500 millones de euros el potencial de inversión de la mano del sector privado.

CÓMO TAIWÁN REFUERZA SU CIBERSEGURIDAD ANTE LAS MANIOBRAS DE CHINA

infobae - El 15 de abril, el presidente Lai Ching-te presentó en CYBERSEC, la mayor conferencia de ciberseguridad de Asia, la nueva estrategia nacional para 2025, en respuesta a las últimas maniobras militares de China en el estrecho de Taiwán. En su discurso, reveló que los sistemas gubernamentales sufrieron 2,4 millones de ciberataques diarios en 2024, el doble que el año anterior. Recientes ataques de ransomware “CrazyHunter” afectaron hospitales, escuelas y empresas, con piratas informáticos chinos identificados como los responsables.

INTELIGENCIA ARTIFICIAL GENERATIVA: OPORTUNIDADES Y RIESGOS PARA LA CIBERSEGURIDAD

Portal Innova - El auge de la Inteligencia Artificial Generativa (IAg) está marcando un antes y un después en el ámbito de la ciberseguridad. Las soluciones de ciberseguridad basadas en IA Generativa permiten automatizar la documentación de incidentes, acelerar la búsqueda y análisis de amenazas, interpretar grandes volúmenes de datos de logs o generar una campaña de sensibilización y cambio cultural. Para incrementar la productividad, las empresas han comenzado a incorporar herramientas como ChatGPT, Copilot, Claude 3 o Gemini.

NEW BILL MANDATES CYBERSECURITY OVERHAUL FOR FEDERAL CONTRACTORS - USA

Fortra - New cybersecurity legislation is coming thick and fast. And for good reason: cyber threats are becoming more sophisticated, systems are becoming more connected, and geopolitical relationships are becoming more fraught. One of the most recent bipartisan legislations – the US Federal Contractor Cybersecurity Vulnerability Reduction Act of 2025 – is designed to modernize cybersecurity standards in the US and protect the country from threats.

CISOS BAND TOGETHER TO URGE WORLD GOVERNMENTS TO HARMONIZE CYBER RULES

Cybersecurity Dive - A letter from the CISOs of 45 powerful global companies could provide crucial backing for world governments looking to reduce cybersecurity regulations and their accompanying hassles for businesses. The CISO letter, sent to members of the Group of Seven nations and the Organization for Economic Cooperation and Development, urges governments to use those high-level forums to “focus on greater alignment of cybersecurity regulations.”

ISC2 UNVEILS COMPREHENSIVE GUIDE FOR CYBERSECURITY IN SATELLITE COMMUNICATIONS

Industrial Cyber - The ISC2 has released a guide for cybersecurity practitioners to support their evaluation of the risks, challenges and use cases for privatized satellite-based communications (SATCOM). Satellite communications (SATCOM) have become more accessible than ever, with consumer mobile devices now able to connect to these networks.

CSIS 2025 SPACE THREAT ASSESSMENT: CYBERATTACKS ON SPACE SYSTEMS PERSIST, TRACKING HARDER AMID INFRASTRUCTURE THREATS

Industrial Cyber - The Center for Strategic & International Studies (CSIS) has released the 2025 Space Threat Assessment, noting that the authors find it increasingly difficult to track the year-over-year number of cyberattacks targeting space systems. Though their numbers differ, some organizations try to keep tallies of cyberattacks by the type of entity and sector targeted, among other criteria.

AS LATIN AMERICA BECOMES THE WORLD'S FAST GROWING REGION FOR NEW CYBERSECURITY ATTACKS, MARKETS LOOK TO AI FOR SOLUTIONS

Latin America Reports - According to a report from the World Bank, Latin America and the Caribbean recently became the world's fastest-growing region for disclosed cyber incidents, with a 25% average annual growth rate in the last decade alone. Furthermore, according to the international financial institution it is also the least protected region.

WEF, UNIVERSITY OF OXFORD PUBLISH CYBER RESILIENCE COMPASS WITH SEVEN PATHWAYS TO BUILD ROBUST CYBERSECURITY ROADMAPS

Industrial Cyber - The World Economic Forum (WEF), in collaboration with the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, released the Cyber Resilience Compass: Journeys Towards Resilience report on Thursday. The practical guide is designed to help organizations develop stronger cyber resilience strategies and navigate today's increasingly complex threat landscape with confidence. Drawing on frontline practices from leading organizations worldwide, the white paper offers actionable insights to support the creation of more effective and resilient cybersecurity roadmaps.

159 CVES EXPLOITED IN Q1 2025 — 28.3% WITHIN 24 HOURS OF DISCLOSURE

The Hacker News - As many as 159 CVE identifiers have been flagged as exploited in the wild in the first quarter of 2025, up from 151 in Q4 2024. "We continue to see vulnerabilities being exploited at a fast pace with 28.3% of vulnerabilities being exploited within 1-day of their CVE disclosure," VulnCheck said in a report shared with The Hacker News. This translates to 45 security flaws that have been weaponized in real-world attacks within a day of disclosure. Fourteen other flaws have been exploited within a month, while another 45 flaws were abused within the span of a year.