DIGI AMERICAS ALLIANCE MEMBERS

PRESENTAN INICIATIVA DE LEY DE CIBERSEGURIDAD - MÉXICO

Congreso Ciudad de México - Con el objetivo de fortalecer el marco normativo en materia de protección de datos personales, el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México presentó en el Congreso local la iniciativa de Ley de Ciberseguridad, respecto del tratamiento de datos personales y la seguridad de la información.

GUERRA DIGITAL: BRASIL FORTALECE CAPACIDADES NO MAIOR EXERCÍCIO CIBERNÉTICO GLOBAL

Defesa em Foco - Entre firewalls e ataques simulados, militares brasileiros participaram do Locked Shields 2025, o maior exercício de defesa cibernética do planeta. Organizado pela OTAN, o treinamento reuniu 41 países em uma simulação realista de guerra digital — e o Brasil foi o único representante da América Latina. Promovido anualmente pelo Centro de Excelência em Defesa Cibernética Colaborativa da OTAN (CCDCOE), com sede em Tallinn, Estônia, o Locked Shields é considerado o mais avançado exercício de guerra cibernética do mundo. Em 2025, 41 nações se uniram para simular ataques digitais coordenados contra infraestruturas críticas, redes governamentais e sistemas militares.

BRASIL E ESPANHA FOMENTAM COOPERAÇÕES SOBRE DEFESA E SEGURANÇA

Forcas Terrestres - Com o objetivo de divulgar a Base Industrial de Defesa (BID) brasileira, o Ministério da Defesa, por meio da Secretaria de Produto de Defesa (Seprod), participou da 4ª Exposição Internacional de Defesa e Segurança da Espanha (Feindef). O evento aconteceu em Madrid, na Espanha, nos dias 12 a 14, e reuniu 92 delegações internacionais com 601 expositores. Para o Secretário de Produtos de Defesa, Heraldo Luiz Rodrigues, a participação nesta exposição foi importante para fomentar futuras parcerias. “Foram feitas diversas reuniões com empresas de alta tecnologia, principalmente da área espacial e cibernética. Todos eles demonstraram interesse em partilhar seu conhecimento com empresas brasileiras, um interesse bastante grande em ter uma participação maior no mercado de defesa”, disse.

INVESTIGAN EL POSIBLE HACKEO DE LOS DATOS DE 50 MIL MILITARES DEL EJÉRCITO: EL ALERTA LLEGÓ POR UN MAIL ANÓNIMO - ARGENTINA

Infobae - El Ejército Argentino denunció ante la Policía Federal un posible hackeo de datos personales de unos 50 mil efectivos de la fuerza, tras recibir un correo electrónico anónimo que afirmaba poseer información de personas vinculadas a la institución. Según informó el Ejército, la denuncia inicial fue presentada el pasado 8 de mayo ante la División Delitos Informáticos de la Policía Federal, y desde entonces se han adoptado medidas preventivas para reforzar la seguridad en los sistemas administrativos.

SUPERINTENDENCIA DE ELECTRICIDAD EMITE REGLAMENTO DE SEGURIDAD CIBERNÉTICA - REPÚBLICA DOMINICANA

RCC Noticias - La Superintendencia de Electricidad (SIE) emitió la resolución que pone en vigencia el “Reglamento de Seguridad Cibernética y de la Información del Subsector Eléctrico en República Dominicana”, después de un proceso de consulta público atendiendo a las normativas que exigen la participación de los actores del subsector en las directrices de cumplimiento obligatorio. La SIE informó que el objetivo del reglamento, es dotar al subsector de “herramientas para salvaguardar los activos tecnológicos críticos del Sistema Eléctrico nacional Interconectado (SENI)”, y fortalecer la capacidad de respuesta “a las amenazas cibernéticas, lo que es fundamental para proteger la seguridad nacional, sobre todo, en infraestructuras críticas como el sistema eléctrico”.

NUEVO CIBERATAQUE SERÍA “UNA DE LAS FILTRACIONES DE DATOS MÁS GRANDES DEL PAIS”, SEGÚN EXPERTO - PARAGUAY

abc.com.py - En conversación con ABC Color este domingo, el experto en ciberseguridad Miguel Ángel Gaspar afirmo que el ciberataque del que fueron victimas varias instituciones del Estado, anunciado hoy por el Ministerio de Tecnologías de la Información y Comunicación (Mitic), es “una de las filtraciones de datos mas grandes del país.”

LATORRE CONSIDERA CLAVE FORTALECER CAPACIDADES PARA LA CIBERSEGURIDAD - PARAGUAY

La Nacion - El presidente de la Cámara de Diputados, Raúl Latorre, indicó que existe una necesidad de seguir fortaleciendo las capacidades en materia de ciberseguridad en el país. Señaló que esta no es una conversación para el futuro, sino que esta es una conversación del presente que se proyecta para el futuro. “La inteligencia artificial, la ciberseguridad, la capacidad de poder generar tranquilidad y seguridad en el ciberespacio en materia de información institucional, en materia de transacciones económicas y financieras son fundamentales para el fortalecimiento de nuestra República y, de hecho, de todos los países del mundo”, sostuvo en conversación con los medios de prensa antes del inicio de la sesión.

DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 15, 2025

IA CONTRA EL CIBERCRIMEN: UNA NUEVA DEFENSA PARA GUATEMALA

Revista Summa - Los ataques cibernéticos continúan en aumento en América Latina, al punto de ser la región de más rápido crecimiento en incidentes cibernéticos divulgados, con una tasa promedio anual del 25 % en la última década, de acuerdo con el informe “Economía de la seguridad para mercados emergentes”, publicado por el Banco Mundial. Guatemala ocupó, en el período 2013/2024, el décimo puesto en cuanto a ataques divulgados. El sector más afectado fue el de la manufactura, seguido por el de la administración pública.

COMISIÓN ESCUCHA OPINIÓN DE EXPERTOS EN CIBERDEFENSA Y ATAQUES A SISTEMAS INFORMÁTICOS - GUATEMALA

Congreso.gob.gt - Con el objetivo de continuar con el análisis y discusión de la iniciativa 6347, ley de ciberseguridad, la Comisión de Asuntos de Seguridad Nacional, que preside el diputado Jorge Mario Villagrán, se reunió de forma híbrida con la mesa técnica de asesores para avanzar y mejorar el contenido para emitir el dictamen respectivo para la aprobación del proyecto de ley. La iniciativa busca desarrollar las capacidades de ciberseguridad y ciberdefensa, así como la tipificación de conductas delictivas, para prevenir, erradicar y sancionar ciberdelitos.

GUATEMALA-US THWART CHINA SPY THREAT

Dialogo Americas - Cooperation with the United States has once again proved strategic in countering the growing threat of China-state sponsored cyberattacks in Latin America. Such was the case recently for Guatemala’s Foreign Ministry (MINEX). “Thanks to close collaboration between both countries, these threats were detected, and the necessary measures were taken to stop them and prevent them in the future,” MINEX told Associated Press on April 30. According to MINEX, Chinese hackers infiltrated its computer systems from September 2022 to February 2025. A U.S. Southern Command’s (SOUTHCOM) comprehensive cybersecurity review of Guatemalan security networks led to the detection of the China-based cyber espionage groups.

CONGRESS FACES PRESSURE TO RENEW CYBER INFORMATION-SHARING LAW - USA

Cybersecurity Dive - A coalition of 52 U.S. organizations urged lawmakers on Tuesday to reauthorize a law that protects cyber threat information that businesses share with the federal government. The Cybersecurity Information Sharing Act, which is set to expire on Sept. 30, creates a system for federal agencies to receive threat indicators from companies and share those indicators with other agencies and companies. The law specifies that companies can share threat information with one another without violating antitrust laws and requires agencies to remove personal information before sharing information. It also prohibits the government from using any shared data to regulate companies.

DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 15, 2025

FIVE YEARS LATER: EVOLVING IOT CYBERSECURITY GUIDELINES

NIST - The passage of the Internet of Things (IoT) Cybersecurity Improvement Act in 2020 marked a pivotal step in enhancing the cybersecurity of IoT products. Recognizing the increasing internet connectivity of physical devices, this legislation tasked NIST with developing cybersecurity guidelines to manage and secure IoT effectively. As an early building block, we developed NIST IR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers, which describes recommended activities related to cybersecurity for manufacturers, spanning pre-market and post-market, to help them develop products that meet their customers' needs and expectations for cybersecurity.

RESEARCH ON CYBER SECURITY IN ENTERPRISE CONNECTED DEVICES

Gov.uk - The UK government is concerned about the security of IoT devices as vulnerable devices can provide a route for hostile actors to attack the IT systems used by businesses. As part of the government's work to address this issue and improve cyber resilience across the UK economy, the government commissioned NCC Group to conduct a vulnerability assessment of some commonly-used enterprise connected devices.

#INFOSEC2025: RANSOMWARE ENTERS 'POST-TRUST ECOSYSTEM,' NCA CYBER EXPERT SAYS

Infosecurity Magazine - The ransomware landscape has entered a "post-trust ecosystem," where fragmented and increasingly mistrustful cybercrime groups operate in a climate of heightened law enforcement scrutiny, according to William Lyne of the UK's National Crime Agency (NCA). The result is a more unpredictable and potentially more perilous threat environment for organizations worldwide. In recent years, a series of high-profile law enforcement takedowns has disrupted some of the most notorious ransomware groups. Now the dust is settling and a cybercrime landscape that's more splintered than ever is emerging.

GROWING CYBER TALENT THROUGH PUBLIC–PRIVATE PARTNERSHIPS

WEF - Public–private partnerships (PPPs) offer a promising approach to cybersecurity workforce development by leveraging the strengths of both the public and private sectors to support skills development, career growth and the creation of sustainable talent pipelines. The Growing Cyber Talent Through Public–Private Partnerships white paper aims to highlight the benefits of PPPs to both sectors, including financial sustainability, market access and infrastructure for cybersecurity education.

POWERING CYBER RESILIENCE IN THE ENERGY SECTOR

WEF - Technology changes are rapidly driving energy-sector growth and changing how energy is produced, moved and stored as demand increases and companies pursue hybridization, asset diversification and partnerships. At the same time, escalating cybersecurity threats against energy infrastructure are making cyber resilience a necessary component of continued growth. Addressing these changing needs requires greater collaboration across the energy sector to build resilience into energy systems.