DIGI AMERICAS ALLIANCE MEMBERS

COMISIÓN RECIBIÓ DETALLES SOBRE PLAN DE CIBERSEGURIDAD DEL MITIC - PARAGUAY

Senado de Paraguay - Durante el encuentro, el ministro Gustavo Villate presentó la Estrategia Nacional de Ciberseguridad 2025–2028, recientemente oficializada mediante el Decreto Nº 3900 del Poder Ejecutivo. Señaló que este instrumento marca un paso trascendental hacia la consolidación de un ecosistema digital más seguro e inclusivo en el país. “El documento consolida el proceso de actualización iniciado en marzo de 2024, tomando como base los avances del Plan Nacional de Ciberseguridad 2017. Surge como respuesta a la necesidad de adaptarse a un entorno digital en constante evolución”, explicó el ministro.

EL CAMINO DIGITAL PARAGUAYO PONE FOCO LA CENTRALIZACIÓN, 5G Y CIBERSEGURIDAD

abc Paraguay - A medida que evoluciona el mercado tecnológico global, Paraguay acelera su agenda digital con inversiones en conectividad, ciberseguridad y centros de datos. Con iniciativas públicas clave y el acompañamiento del sector privado, el país busca posicionarse como un actor competitivo en la economía digital regional.

DOS JORNADAS CLAVES PARA LA CIBERSEGURIDAD NACIONAL Y EL DESPLIEGUE DE LA NUEVA LEY - CHILE

trendtic.cl - Con un importante anuncio por parte de la Agencia Nacional de Ciberseguridad (ANCI) sobre el inicio del proceso de calificación de Operadores de Importancia Vital (OIV), concluyeron este viernes en Puerto Varas las dos jornadas de “Patagonia Ciber 2025”. Este primer gran encuentro nacional de ciberseguridad, organizado por Fundación País Digital y la ANCI, congregó a más de 500 personas por jornada, incluyendo a destacados líderes económicos, empresariales y autoridades, para abordar los desafíos y avances en la materia bajo el nuevo marco legal chileno.

EXÉRCITO CONSOLIDA SEGURANÇA CIBERNÉTICA COM DATA CENTER EM SÃO PAULO - BRASIL

LRCA - O 3° Centro de Telemática de Área (3° CTA) inaugurou um data center no dia 29 de maio, na capital paulista. Nomeado Data Center Marechal Rondon, o centro de processamento de dados reforça as capacidades do Data Center Coronel Ricardo Franco, localizado em Brasília (DF), e consolida a segurança cibernética da Força Terrestre. O Data Center Marechal Rondon será um pilar no suporte à tomada de decisão estratégica, fornecendo dados em tempo real, análises avançadas e suporte informacional confiável ao Alto Comando do Exército Brasileiro. Sua infraestrutura permite o intercâmbio seguro e rápido de informações entre diferentes níveis operacionais e institucionais.

BRASIL GANHA PRIMEIRO CENTRO INTEGRADO DE INTELIGÊNCIA CIBERNÉTICA

Canção Nova - O primeiro Centro Integrado de Inteligência Cibernética do país foi inaugurado na Cidade Administrativa em Minas Gerais. A intenção é monitorar ameaças feitas no ambiente digital e ajudar a prevenir ataques em instituições de ensino.

GOVERNO SUSPENDE SETE SITES DE APOSTAS POR FALHA EM SEGURANÇA DIGITAL; VEJA LISTA - BRASIL

g1 - A Secretaria de Prêmios e Apostas do Ministério da Fazenda (SPA/MF) suspendeu nesta sexta-feira (30) sete operadoras de apostas esportivas de quota fixa e todos os seus respectivos sites. As empresas descumpriram exigência da regulamentação ao não entregarem relatórios obrigatórios de avaliação de segurança dos sistemas. Com a decisão, os sites ficam proibidos de oferecer apostas, aceitar depósitos ou cadastrar novos usuários no Brasil, até que apresentem os documentos exigidos. Caso continuem operando, serão multadas em R$ 40 mil por dia.

ALERTAN POR AUMENTO DE CIBERATAQUES CONTRA INFRAESTRUCTURA CRÍTICA EN MÉXICO

almomento - En México, las infraestructuras críticas están cada vez más expuestas a ciberataques que podrían paralizar servicios esenciales. Expertos en seguridad informática advierten que la falta de actualizaciones en el software, los vacíos normativos y la escasez de especialistas han convertido al país en un terreno vulnerable para actores maliciosos. Durante el último año, se ha registrado un aumento en los intentos de intrusión a redes estratégicas como sistemas eléctricos, plantas de tratamiento de agua y plataformas hospitalarias. Estos ataques buscan interrumpir operaciones, manipular datos o provocar daños físicos mediante la explotación de brechas en la seguridad digital.

ATENCIÓN: ALERTAN CIBERATAQUES POR ELECCIÓN DEL PODER JUDICIAL EN MÉXICO

dplnews - Por primera vez en México habrá una elección del Poder Judicial (jueces y magistrados) el próximo 1 de junio, y especialistas en ciberseguridad ya advirtieron de posibles ataques, tanto a las instituciones involucradas en el proceso como a los propios ciudadanos y ciudadanas. De acuerdo con la firma de ciberseguridad Netscout Systems, ha habido un incremento del 218 por ciento en ataques de Denegación de Servicio Distribuido (DDoS) contra infraestructuras críticas del país, coincidiendo con la coyuntura electoral.

REGULACIÓN EN CIBERSEGURIDAD ES TAREA PENDIENTE EN MÉXICO: AMCS

El Economista - A pesar del creciente volumen de información personal que manejan las instituciones públicas en México y del surgimiento de nuevas iniciativas legislativas en materia digital, el país aún carece de un marco normativo integral en ciberseguridad. Así lo advirtió Ernesto Ibarra, coordinador de la Alianza México Ciberseguro (AMCS) y presidente de la Asociación Mexicana de Ciberseguridad y Derecho Digital (Amcid), en entrevista con El Economista.

CIBERSEGURIDAD FINANCIERA EN EL SECTOR BANCARIO - MÉXICO

idc - La seguridad digital es un tema cada vez más relevante, y cuando hablamos de dinero, el tema es aún más importante, por ello, el Gobierno de México y la banca están apostando por la ciberseguridad financiera. Al respecto, el presidente saliente de la Asociación de Bancos de México (ABM), Julio Carranza Bolívar, mencionó en la 88 Convención Bancaria celebrada en Nayarit, que en la actualidad se procesan casi 21 mil millones de transacciones al año a través del sistema bancario, es decir, "2.4 millones de operaciones por hora, 675 por segundo".

CIBERSEGURIDAD DEBE CONTEMPLAR LA PROTECCIÓN DE DERECHOS HUMANOS - MEXICO

Gaceta UNAM - Ante la llegada de neurotecnologías que prometen ayudar contra la depresión o implantar chips en el cerebro para conectarlos a computadoras, es importante ser conscientes de la necesidad de proteger nuestros datos biométricos (que incluyen las ondas cerebrales) para evitar un mal uso de ellos. Así lo recomendó Anahiby Becerril Gil, académica de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la UNAM, quien precisó que cada vez más se ha normalizado en la sociedad la “entrega” de este tipo de información –nuestro rostro, voz, iris y huella digital– al usar los llamados equipos inteligentes (celulares, relojes, tabletas, audífonos), sin cuestionar a quién se envía, para qué se usa, cuánto tiempo la conservarán o con qué fines.

¿CUÁLES SON LOS RETOS QUE ENFRENTAN LOS GOBIERNOS ANTE LA DIGITALIZACIÓN Y PROTECCIÓN DE DATOS? ESTO SEÑALAN EXPERTOS

Infobae - Los gobiernos y empresas enfrentan el desafío de mantener el control sobre sus datos y tecnologías en un entorno globalizado. La soberanía digital implica desarrollar capacidades locales en infraestructura, software y regulación para proteger la autonomía tecnológica y cumplir con normativas internacionales. Los gobiernos buscan modernizar sus servicios mediante la digitalización, pero enfrentan obstáculos como la resistencia al cambio, limitaciones presupuestarias y la necesidad de garantizar la inclusión digital.

WHY CYBER RESILIENCE SHOULD BE A TOP PRIORITY FOR FREIGHT FORWARDERS

WEF - Freight forwarders are accelerating digitalization to boost efficiency, but this also increases vulnerability to cyber threats. Ransomware attacks show how even short disruptions can ripple through supply chains, especially impacting small and medium-sized forwarders. FIATA is leading efforts to strengthen cyber resilience through practical guidance, training, and tools for the global freight forwarding community.

CYBER ATTACKS AND RANSOMWARE RISE GLOBALLY IN EARLY 2025

digwatch - Cyber attacks have surged by 47% globally in the first quarter of 2025, with organisations facing an average of 1,925 attacks each week. Ransomware activity alone has soared by 126% compared to last year. Attackers are no longer just encrypting files but now also threaten to leak sensitive data unless paid — a tactic known as dual extortion. Instead of operating as large, centralised gangs, modern ransomware groups are smaller and more agile, often coordinating through dark web forums, making them harder to trace.