



DIGI

AMERICAS

LATAM

CISO

INSIGHTS

JUNE 20, 2025

DIGI AMERICAS ALLIANCE MEMBERS



PANAMÁ FORMALIZA LA CREACIÓN DEL CENTRO DE CIBERSEGURIDAD ESTATAL

La Estrella - Panamá avanza hacia la consolidación de su Centro de Control de Ciberseguridad, destacó el administrador de la Autoridad de Innovación Gubernamental, Adolfo Fábrega. El pasado 11 de junio, el presidente de la República, José Raúl Mulino, firmó el Decreto Ejecutivo No. 53, que formaliza la implementación del centro para la protección de los servicios, la información y la infraestructura tecnológica del Estado. "Ya tenemos la adjudicación del primer componente de este centro", indicó Fábrega; se trata de un equipo de seguridad que evaluará la vulnerabilidad de cada institución del Estado, el cual tiene un coste estimado de \$500.000.

COSTA RICA TRAMITA INGRESO A ORGANISMO DE CIBERSEGURIDAD REGIONAL

Prensa Latina - El Ministerio de Ciencia, Tecnología y Telecomunicaciones suscribió el documento para integrar esa iniciativa que ofrece a países de la región opciones de respuesta ante incidentes cibernéticos, y contempla aspectos de prevención y eficacia de políticas, añadió el diario El Observador. "Celebramos esta gestión hacia el LAC4 como parte de las acciones para el robustecimiento de las capacidades nacionales en ciberseguridad a través de alianzas regionales y globales", declaró el viceministro de esa cartera, Orlando Vega.

GOBIERNO DE PEÑA LANZÓ OFICIALMENTE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD - PARAGUAY

La Nacion - "Mi deber como presidente es que cada institución del Estado proteja los datos y derechos de los ciudadanos con la misma seriedad con la que protegen sus recursos físicos", manifestó el presidente de la República, Santiago Peña, durante el lanzamiento oficial de la Estrategia Nacional de Ciberseguridad 2025-2028. "Hoy damos un paso decisivo como país, con nuestra Estrategia Nacional de Ciberseguridad, donde queremos reafirmar nuestro compromiso, no solo con la tecnología, sino principalmente con la gente. El Estado tiene que ser un escudo, no puede ser el riesgo", dijo el mandatario.

"ESTAMOS LUCHANDO CON FUSILES DE MADERA CONTRA DRONES LÁSER", DICE EXPERTO ANTE EXPOSICIÓN DE PARAGUAY EN GUERRA DIGITAL

El Nacional - Paraguay sufre una ola de ciberataques que expuso datos sensibles de instituciones públicas. El experto en delitos informáticos Sergio Mendoza advierte que el país está indefenso, sin leyes ni tecnología para enfrentar esta amenaza.

DATA CENTERS NO BRASIL: DESAFIOS, OPORTUNIDADES E POLÍTICAS PÚBLICAS PARA UM FUTURO DIGITAL

Brasil Pais Digital - Os data centers, ou centros de processamento de dados, são instalações físicas que constituem os pilares essenciais da infraestrutura digital contemporânea. Eles abrigam servidores, dispositivos de armazenamento e redes, sendo cruciais para o processamento e armazenamento massivo de dados digitais. Em uma era definida pela Sociedade da Informação e pela economia digital, na qual a informação digital e a internet são centrais, os data centers suportam desde buscas online e transações bancárias até aplicações avançadas em Saúde, Agronegócio, Indústria e Cidades. Com a explosão da demanda impulsionada pela Inteligência Artificial (IA) e a crescente digitalização, a necessidade por infraestrutura de data centers aumenta exponencialmente.

ABERTAS INSCRIÇÕES PARA SEMINÁRIO NO STF SOBRE SEGURANÇA CIBERNÉTICA NO JUDICIÁRIO - BRASIL

STF - Estão abertas as inscrições para o II Seminário Internacional de Segurança Cibernética nas Cortes Superiores, que será realizado em 25 de junho, na sala de sessões da Segunda Turma do Supremo Tribunal Federal (STF). O evento integra a Semana de Segurança da Informação e Integridade Digital do STF, que ocorrerá de 23 a 27 de junho. O seminário é direcionado a representantes dos tribunais superiores, órgãos do Judiciário brasileiro e internacional, conselhos da Justiça, setor privado, academia e instituições parceiras.

EL RANSOMWARE TODAVÍA DOMINA EL PANORAMA DE CIBERATAQUES EN AMÉRICA LATINA: 8 DE CADA 10 INCIDENTES AFECTAN AL SECTOR FINANCIERO

Clarín - "El espíritu innovador y emprendedor de América Latina no viene con una preocupación por la ciberseguridad". Esta es una de las conclusiones de un nuevo relevamiento sobre las ciberdefensas del sector financiero de la región, donde se registró la mayor cantidad de casos de ransomware, un tipo de ataque que encripta la información para extorsionar a cambio de un rescate. El paper fue publicado este martes por la Universidad de Duke y Digi Americas, una organización enfocada en la ciberseguridad del continente americano. Además de enfocarse en el impacto del ransomware en el sector financiero, también le dedica unas páginas al phishing, los troyanos bancarios, ataques a terceros y explotación de vulnerabilidades.

CIBERDELINCUENTES ADOPTAN IA AGÉNTICA PARA LANZAR ATAQUES SIN INTERVENCIÓN HUMANA DIRECTA

Newsinamerica - Guatemala enfrenta una creciente sofisticación en el panorama de amenazas digitales, con un aumento sostenido en los reportes de incidentes de ciberseguridad. Según el Boletín de Ciberseguridad del GT-CERT 2024, se registraron múltiples eventos de compromiso, incluyendo campañas de phishing dirigidas, intentos de explotación de vulnerabilidades conocidas y ataques de ransomware contra entidades públicas y privadas. Estas amenazas ponen en evidencia la necesidad de reforzar la postura de ciberseguridad a nivel nacional, especialmente en sectores críticos como el financiero, educativo y gubernamental, donde la digitalización avanza aceleradamente.

AMÉRICA LATINA CREARÁ SU PROPIO MODELO DE INTELIGENCIA ARTIFICIAL: LATAM-GPT

Forbes - Una docena de países de América Latina unieron esfuerzos para crear el primer lenguaje de inteligencia artificial de gran tamaño que entiende las particularidades de la región y cuya primera versión será lanzada en septiembre, anunciaron el martes autoridades chilenas.

NIST FLAGS RISING CYBERSECURITY CHALLENGES AS IT AND OT SYSTEMS INCREASINGLY CONVERGE THROUGH IOT INTEGRATION - USA

Industrial Cyber - The U.S. National Institute of Standards and Technology (NIST) has observed in a discussion essay a growing convergence between OT (operational technology (OT) and IT, driven by the rise of the Internet of Things (IoT) and internet-connected equipment that were once isolated. OT infrastructure covers programmable systems and devices that directly interact with or control the physical environment.

THIRD-PARTY CYBER ATTACKS PUT SPOTLIGHT ON CONTINGENT BUSINESS INTERRUPTION COVERAGE

Insurance Business Magazine - A string of high-profile cyber attacks involving third-party software vendors last year has forced organizations to take a hard look at their contingent business interruption (CBI) coverage. According to one wholesale broker specializing in cyber, businesses' vulnerability to third-party outages was exemplified by two events in 2024: the Change Healthcare breach and the CDK Global attack.

HOW ENERGY AND MANUFACTURING CAN STAY AHEAD OF CYBER THREATS AND PROTECT THEIR TECH

WEF - Operational technology (OT) environments in the energy and manufacturing sectors are often outdated, poorly segmented and generally perceived as insecure. Limited internal resources and scarce cybersecurity expertise mean companies are increasingly relying on outsourcing to strengthen OT security. The rapid adoption of artificial intelligence is not only increasing energy demand but also intensifying cybersecurity risks.