DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 23, 2026

DIGI AMERICAS ALLIANCE MEMBERS

PANAMÁ PRESENTA EL NUEVO CENTRO DE MONITOREO DE CIBERSEGURIDAD

SEGURILATAM - Francisco Guinard, subadministrador de la Autoridad Nacional para la Innovación Gubernamental (AIG), ha presentado el nuevo Centro de Monitoreo de Ciberseguridad de Panamá. Esta iniciativa busca fortalecer la capacidad del Estado para detectar, prevenir y responder a amenazas digitales. De esta manera, el país contará con mayor visibilidad sobre los riesgos en tiempo real y podrá anticiparse a posibles incidentes. “El objetivo es evitar los ataques o, en caso de que ocurran, contenerlos antes de que se conviertan en un riesgo mayor para los datos de los ciudadanos”, explica el subadministrador.

PANAMÁ DESARROLLA ESTRATEGIA PARA EXPORTACIÓN DE SERVICIOS MODERNOS

Revista E&N - Panamá lanzó la Estrategia Nacional de Exportaciones de Servicios Modernos de Panamá (ENESM-PA 2026), una hoja de ruta que busca potenciar sectores intensivos en conocimiento, tecnología y talento humano. La iniciativa, liderada por el Ministerio de Comercio e Industrias (MICI), marca el paso del diseño a la ejecución tras seis meses de trabajo técnico y coordinación con el sector privado y académico.

COMISIÓN DE LA CÁMARA DE DIPUTADOS APRUEBA REFORMAS PARA PROTEGER A NIÑOS, NIÑAS Y ADOLESCENTES EN INTERNET – MÉXICO

infobae - La Comisión de Derechos de la Niñez y Adolescencia de la Cámara de Diputados aprueba reformas a la Ley General de los Derechos de las Niñas, Niños y Adolescentes con el objetivo de fortalecer la protección contra el ciberacoso, la violencia digital y garantizar la seguridad de los datos personales de los menores de edad en entornos digitales. Esta modificación legal responde al crecimiento acelerado de riesgos en plataformas digitales y busca establecer medidas directas para prevenir contenido dañino y proteger la identidad digital.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 23, 2026

POLICÍA CIBERNÉTICA ALERTA SOBRE LAS OFERTAS LABORALES FALSAS EN REDES SOCIALES - MÉXICO

El Heraldo de México - Especialistas en seguridad digital han encendido las alertas en México ante el creciente número de ofertas laborales falsas que circulan en redes sociales y otras plataformas digitales. Estas estafas, que prometen sueldos elevados y prestaciones superiores a la ley, buscan aprovecharse de la necesidad económica de los buscadores de empleo, según advierten expertos en ciberseguridad. La proliferación de estos anuncios engañosos representa un riesgo significativo para la población. Los delincuentes utilizan tácticas muy atractivas para captar la atención de quienes buscan una oportunidad laboral. Ofrecen sueldos que pueden ascender a 8,000 pesos semanales para roles como edecanes, junto con beneficios que superan lo establecido por la ley.

CIBERSEGURIDAD MARÍTIMA: TERMINAL PORTUARIO VALPARAÍSO AVANZA EN GESTIÓN DE RIESGOS DIGITALES Y PROTECCIÓN DE DATOS PORTUARIOS - CHILE

g5noticias - Terminal Portuario Valparaíso (TPV) anunció la implementación de la Circular Marítima DGTM y MM O-75/006, normativa que establece nuevas disposiciones para la gestión de riesgos cibernéticos marítimos y la protección de la información en instalaciones portuarias. Con este hito, TPV consolida su posicionamiento como terminal marítimo de altos estándares de cumplimiento, dando continuidad a los avances impulsados por la Circular Marítima O 75/005, que establece la implementación de un sistema de gestión del riesgo cibernético-marítimo alineado con la normativa vigente y las mejores prácticas internacionales.

INFRAESTRUCTURA DIGITAL YA ES CRÍTICA PARA CHILE: ACTI PIDE DESTRABAR INVERSIÓN EN DATA CENTERS Y CLOUD

dpl news - En Chile, la infraestructura digital dejó de ser un “tema TI” para convertirse en un componente crítico de continuidad operacional del país. Data centers, servicios cloud, conectividad y ciberseguridad hoy sostienen pagos, logística, telecomunicaciones, servicios públicos, salud y operación industrial. Cuando esa base falla, se interrumpen servicios esenciales y se afecta directamente el desarrollo de la economía digital.

MARINHA REFORÇA CAPACIDADE DE DEFESA NO AMBIENTE DIGITAL - BRASIL

Defesa Net - A Marinha do Brasil (MB) tem ampliado sua atuação no domínio cibernético diante da crescente importância do ambiente digital nos conflitos contemporâneos. Nesse contexto, a Força ativou, em agosto de 2025, o Esquadrão de Guerra Cibernética (EsqdGCiber), iniciativa que fortalece as capacidades de Defesa Cibernética e a proteção de sistemas estratégicos navais. Guerras contemporâneas não se limitam ao emprego de tropas e armamentos convencionais; elas também se desenvolvem no ambiente digital, onde sistemas, redes e informações se tornam alvos estratégicos. Nesse cenário, a estratégia militar moderna passou a considerar o chamado “quinto domínio operacional” — o ciberespaço ou domínio cibernético —, que se soma aos quatro domínios tradicionais: terra, mar, ar e espaço.

DIGI AMERICAS LATAM CISO

INSIGHTS

APRIL 23, 2026

ANTHROPIC INVESTIGA ACCESO NO AUTORIZADO A SU MODELO DE IA MYTHOS

CR Hoy - La empresa estadounidense de inteligencia artificial Anthropic anunció el martes que investiga un acceso no autorizado a su poderoso modelo Mythos, que la compañía teme se puede convertir en una herramienta valiosa para los hackers. Anthropic dijo semanas atrás que limitó inicialmente el lanzamiento de Mythos a 40 grandes firmas tecnológicas para darles ventaja a la hora de corregir vulnerabilidades de ciberseguridad antes de que pudieran ser explotadas por atacantes. Según la agencia financiera Bloomberg, un pequeño grupo de usuarios en un foro privado en línea obtuvo acceso al modelo mediante el sistema informático reservado para proveedores externos de Anthropic.

IDB GROUP ADVANCES REGIONAL COOPERATION AT ONE CARIBBEAN MINISTERIAL DIALOGUE

IDB - The Inter-American Development Bank Group (IDB Group) launched three key regional initiatives on cybersecurity, capital market integration and fiscal policy under its regional program ONE Caribbean, that aims to foster long-term stability and growth in the Caribbean. The new actions were presented during the ONE Caribbean Ministerial Dialogue in Port of Spain, Trinidad and Tobago, a high-level gathering that marked the program’s two-year milestone. Through this leadership dialogue, IDB Governors and regional partners deliberated on emerging priorities for shaping the next phase of the program.

SEEING THE CYBER IN ECONOMIC STATECRAFT - USA

War on the Rocks - Americans lost nearly $21 billion to cybercrime in 2025, a new record for cyber-enabled economic losses. Private sector losses to malicious cyber activity regularly exceed $200 billion in a given year. Alongside criminal groups, state-sponsored hackers are increasingly targeting America’s pocketbook. Neither the economic sphere nor cyberspace are classic terrestrial warfighting domains. Yet war is being actively waged through both realms and national cyber security is vital to the prosperity and protection of today’s hyperconnected economy. China is both the greatest economic threat and the most active and persistent cyber threat to the United States. Both its economic and cyber statecraft campaigns reach deep into America’s government, private sector, and critical infrastructure. These two efforts overlap: Cyber espionage, digital theft, and supply chain compromises are key pillars of China’s strategy to undermine the U.S. economy. Addressing this challenge requires marshaling economic and cyber power into cohesive, coordinated campaigns.

UK CYBER AGENCY HANDLING FOUR MAJOR INCIDENTS A WEEK AS NATION-STATE ATTACKS SURGE

The Record - Britain's cybersecurity chief warned Tuesday that the country is handling four nationally significant cyber incidents every week, with the majority now traced back to hostile foreign governments rather than criminal hackers, as the government unveiled a £90 million (about $121.48 million) package to bolster the country's digital defences. Richard Horne, chief executive of the National Cyber Security Centre (NCSC), told the annual CYBERUK conference in Glasgow that while the incident rate had held relatively steady since he first disclosed the figure last October, the origin of those attacks had shifted dramatically.