DIGI AMERICAS ALLIANCE MEMBERS

Apple AppGate aws Batuta Chainguard CHECK POINT CISCO CLOUDFLARE
CROWDSTRIKE fluidattacks Google kriptos LUMU netskope paloalto NETWORKS Schneider Electric
SISAP Sistemas Aplicativos SOPHOS TANIUM tenable Trellix TrendAI whalemate zscaler

BANCA Y TELECOMUNICACIONES VEN OPORTUNIDADES EN LA ESTRATEGIA DE IA DE PANAMÁ

La Estrella de Panamá - La presentación de la Estrategia Nacional de Inteligencia Artificial (IA) por parte de la Senacyt generó un amplio respaldo en el sector privado panameño. Voces de la banca, las telecomunicaciones y la ciberseguridad coinciden en que el país tiene una oportunidad única para consolidarse como un hub digital en las Américas, complementando su rol logístico y financiero. Desde las telecomunicaciones se advirtió que la IA es tanto una oportunidad como una amenaza: Panamá mide una madurez cercana al 46% en ciberseguridad, mientras que la banca alcanza alrededor del 65%, brechas que aún deben cerrarse fortaleciendo la gobernanza de datos y la protección de información sensible.

PANAMÁ ANALIZA MECANISMOS PARA APLICAR ITBMS A SERVICIOS DIGITALES

AIG - El administrador general de la Autoridad Nacional para la Innovación Gubernamental (AIG), Adolfo Fábrega, explicó los alcances de la iniciativa que busca aplicar el 7% de ITBMS a determinados servicios digitales utilizados en Panamá. La propuesta busca establecer condiciones más equitativas entre los comercios establecidos en el país y las plataformas internacionales que ofrecen servicios digitales a consumidores locales, como plataformas de streaming, servicios de música, herramientas de productividad, correo electrónico y otros servicios corporativos en la nube. El escenario ideal es que las propias plataformas incorporen el 7% en la factura y remitan el impuesto al fisco panameño; como alternativa, se analiza un mecanismo mediante los medios de pago electrónicos, en coordinación con las entidades bancarias.

ANCI PRESENTA RESUMEN EJECUTIVO DE LA CONSULTA PÚBLICA POR NORMATIVA BÁSICOS DE LA CIBERSEGURIDAD - CHILE

ANCI - La Ley Marco de Ciberseguridad establece que, para emitir nuevas medidas de seguridad, la Agencia Nacional de Ciberseguridad (ANCI) debe someterlas a consulta pública. Por ello, en junio realizó una consulta pública sobre seis controles que la ANCI denomina los “9 básicos de la ciberseguridad”. Los resultados, basados en la participación con observaciones de cientos de ciudadanos, se resumen en un documento descargable en formato PDF disponible en el sitio de la Agencia.

DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 27, 2026

ENTEL IMPULSA UNA AGENDA NACIONAL PARA QUE BOLIVIA FORTALEZCA LA CIBERSEGURIDAD

MOPSV - Proteger la información y los sistemas digitales se ha convertido en una prioridad para gobiernos, empresas y ciudadanos en el mundo; en este contexto, el ministro de Obras Públicas, Mauricio Zamora, impulsa actividades para que Bolivia avance en la construcción de una agenda nacional de ciberseguridad. En esa línea, Entel presentó el proyecto “Bolivia Cibersegura 2026”, un espacio que reunió a especialistas, instituciones del sector público y privado y expertos nacionales e internacionales para fortalecer las capacidades del país frente a los riesgos y amenazas del entorno digital. La empresa estatal aporta conectividad, infraestructura y soluciones de seguridad; “la ciberseguridad debe abordarse como una agenda de país, construida desde la cooperación y la complementación institucional”, aseguró el gerente general de Entel, Jorge Del Solar.

MINISTRO VILLATE DETALLA LA PROYECCIÓN DE SOBERANÍA TECNOLÓGICA Y EL FORTALECIMIENTO DE LA CIBERSEGURIDAD - PARAGUAY

MITIC - El ministro de Tecnologías de la Información y Comunicación, Gustavo Villate, detalló la proyección del país en materia de soberanía tecnológica y el fortalecimiento de la ciberseguridad. Para articular el desarrollo tecnológico, el gobierno avanza en la creación del Distrito Innova, un parque tecnológico enfocado 100% en el ámbito digital que integrará la investigación científica, la academia y el sector público y privado. En materia de ciberseguridad, la estructura de seguridad digital se divide en la ciberdefensa, bajo el Ministerio de Defensa, y el ámbito civil, público y privado, gestionado por la Dirección General de Ciberseguridad del MITIC, cuyo Centro de Respuesta a Incidentes Cibernéticos (CERT) pasó a operar en un esquema de monitoreo continuo de 24 horas, los 7 días de la semana.

ANPD AVALIA COMO PLATAFORMAS DIGITAIS ATUAM PARA PREVENIR CONTEÚDOS CRIMINOSOS E PROTEGER CRIANÇAS E MULHERES NA INTERNET - BRASIL

gov.br - A Agência Nacional de Proteção de Dados (ANPD) iniciou ações de monitoramento das principais plataformas digitais, lojas de aplicativos e ferramentas de Inteligência Artificial generativas para verificar se estão adotando medidas para cumprimento das obrigações estabelecidas pelo Marco Civil da Internet e pelo Estatuto Digital da Criança e Adolescente (ECA Digital). As empresas começaram a ser notificadas e deverão responder em até dez dias úteis. O objetivo é verificar se as plataformas adotam mecanismos adequados para prevenir e impedir a circulação de conteúdos criminosos ou ilícitos, com especial atenção a riscos que impactem crianças, adolescentes e mulheres no ambiente digital.

CRC PUBLICA ESTUDIO SOBRE CIBERSEGURIDAD EN LA ERA DE LA IA Y PRESENTA HOJA DE RUTA PARA EL SECTOR DE TELECOMUNICACIONES - COLOMBIA

CRC - La Comisión de Regulación de Comunicaciones (CRC) publicó el estudio “Ciberseguridad en la era de la IA: Prioridades estratégicas y hoja de ruta para el sector de telecomunicaciones”, una guía integral orientada a fortalecer la resiliencia digital de las redes de comunicaciones en Colombia y a comprender los riesgos emergentes asociados a la inteligencia artificial. El informe aborda el panorama de amenazas mediante cinco ejes estratégicos: la crisis dual de la IA, las infraestructuras críticas, la seguridad cuántica, la cibercultura y el entrenamiento en ciberseguridad, e incluye un mapa de navegación hacia marcos y estándares internacionales para los proveedores de redes y servicios.

DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 27, 2026

EE.UU. DESBARATÓ UNA RED DE CIBERESPIONAJE CHINO QUE ATACÓ A LA NASA, LA RESERVA FEDERAL Y EL SENADO

Yahoo Noticias - El Departamento de Justicia de Estados Unidos y el FBI anunciaron la incautación de dominios web vinculados a dos plataformas de piratería complementarias, conocidas como QScan y QTRouter, creadas según Washington por un grupo respaldado por el Gobierno de China y empleadas en ciberataques contra la NASA, la Reserva Federal, el Senado y múltiples carteras del Ejecutivo estadounidense. Según la investigación, QScan se utilizó para escanear e infectar miles de dispositivos IoT, mientras que el proveedor QTFY ofrecía servicios de ciberataque a clientes vinculados al Ministerio de Seguridad del Estado chino y al Ejército Popular de Liberación desde al menos 2018.

A TALE OF TWO SOCS: INSIGHTS FROM TWO RED TEAM ASSESSMENTS - USA

CISA - The Cybersecurity and Infrastructure Security Agency conducted two simultaneous red team assessments of critical infrastructure organizations using similar tradecraft, but observed sharply different defensive outcomes. In one organization the team gained access to multiple workstations, elevated privileges over the domain and moved laterally to sensitive business systems and cloud resources undetected, while in the second, defenders quickly detected the initial compromise and quarantined the affected systems. CISA attributes the difference to factors such as alert triage, shared visibility across security tools, and hardened Active Directory, cloud token and endpoint-management controls, and urges critical infrastructure organizations to apply the advisory's mitigations.

INTERPOL GOLPEA EL CIBERFRAUDE GLOBAL Y EL BLANQUEO DEL CRIMEN ORGANIZADO DE ÁFRICA OCCIDENTAL

Escudo Digital - Una acción policial coordinada a escala internacional asestó un severo golpe a las principales redes del crimen organizado originarias de África Occidental. Desarrollada entre noviembre de 2025 y junio de 2026 bajo el nombre de Operación Jackal IV, la iniciativa contó con la participación de fuerzas de seguridad de 22 países y se saldó con 58 detenciones —entre ellas 17 en Argentina— y 263 sospechosos identificados, tras desmantelar redes dedicadas a fraudes con criptomonedas, estafas románticas, compromisos de correo corporativo y blanqueo de capitales vinculadas a organizaciones como Black Axe.

HACKERS CHINOS DUPLICARON SUS CIBERATAQUES TRAS INTEGRAR DEEPSEEK EN SUS OPERACIONES

Infobae - Grupos de hackers vinculados al régimen chino más que duplicaron el volumen de sus ciberataques desde que incorporaron DeepSeek y otros modelos de inteligencia artificial de código abierto a sus operaciones, según un informe de la firma taiwanesa TeamT5, que rastreó el uso de estas herramientas en distintas fases de las campañas de intrusión. Los investigadores coincidieron en que DeepSeek se ha convertido en la opción predilecta de los hackers chinos por su rendimiento elevado, su bajo costo de operación y controles de seguridad más permisivos que los de sus competidores, lo que les ofrece un margen de maniobra mucho más amplio que los modelos occidentales.