DIGI AMERICAS ALLIANCE MEMBERS

Apple aws Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks
Google kriptos LUMU netskope paloalto NETWORKS Resecurity
Schneider Electric SISAP Sistemas Aplicativos Strike Telefónica tenable Trellix TREND MICRO

REPÚBLICA DOMINICANA | INDOTEL IMPULSA FORMACIÓN EN CIBERSEGURIDAD TRAS MIL MILLONES DE INTENTOS DE CIBERATAQUES EN UN AÑO

DPL News - El presidente del Consejo Directivo del Instituto Dominicano de las Telecomunicaciones (Indotel), Guido Gómez Mazara, afirmó que el órgano regulador está estimulando procesos de formación en materia de ciberseguridad para que República Dominicana siga siendo un país seguro en términos tecnológicos y en la protección de los datos digitales.

PANAMÁ REFUERZA SU DEFENSA DIGITAL ANTE LA OLA DE CIBERATAQUES GLOBALES

La Estrella de Panama - Frente al incremento de ciberataques a nivel mundial, Panamá avanza en la protección de sus sistemas críticos con soluciones de ciberseguridad, incluyendo automatización e inteligencia artificial, para garantizar continuidad operativa y cumplimiento normativo. La amenaza cibernética se intensifica. En los últimos meses, ataques sofisticados han sacudido aeropuertos, fábricas y la seguridad de millones de usuarios. Los hackers aprovechan inteligencia artificial y técnicas avanzadas de ingeniería social, ampliando la superficie de ataque a sectores críticos como educación, energía y aviación.

DEBATEDORES ELOGIAM E FAZEM SUGESTÕES PARA O MARCO LEGAL DA CIBERSEGURANÇA - BRASIL

Agência Senado - Em audiência pública promovida pela Frente Parlamentar de Apoio à Cibersegurança e Defesa Cibernética na tarde desta terça-feira (4), especialistas elogiaram e fizeram sugestões ao projeto do Marco Legal da Cibersegurança (PL 4.752/2025). O autor do projeto é o senador Esperidião Amin (PP-SC), que também é o presidente da frente parlamentar. Foi ele quem dirigiu a audiência. O senador informou que o projeto ainda aguarda a designação de relator na Comissão de Constituição e Justiça (CCJ). E sugeriu que a relatoria seja entregue a um senador membro da frente.

¿ANATEL ASUMIRÁ LA REGULACIÓN DE LA CIBERSEGURIDAD EN BRASIL?

DPL News - Sin margen presupuestario para crear una nueva autarquía, el Gabinete de Seguridad Institucional (GSI) de la Presidencia de Brasil decidió proponer que la Agencia Nacional de Telecomunicaciones (Anatel) asuma el papel de órgano central de la política de ciberseguridad del gobierno federal. El cambio figura en la nueva versión del anteproyecto de ley que se debate en el Comité Nacional de Ciberseguridad (CNCiber). El ministro jefe del GSI, general Marcos Antonio Amaro dos Santos, explicó que la iniciativa busca dar alcance nacional a la Política y a la Estrategia de Ciberseguridad —aprobadas en 2023 y 2025, respectivamente—.

COMO SOCS ENFRENTAM AS AMEAÇAS CIBERNÉTICAS NO BRASIL

Computer Weekly - Segundo dados da Febraban, 100% dos bancos brasileiros consideram a segurança da informação como prioridade máxima, refletindo uma tendência que se estende para outros setores críticos da economia. Paralelamente, o setor de TI nacional cresce a taxas superiores a 9% ao ano, incluindo investimentos em segurança, monitoramento e infraestrutura digital. Os SOCs não apenas monitoram e detectam incidentes em tempo real, mas também estruturam processos de resposta rápida e coordenada, reduzindo impactos financeiros e reputacionais. No entanto, manter um SOC interno robusto exige investimentos elevados em tecnologia e especialistas, criando espaço para o crescimento do modelo SOCaaS (SOC como Serviço), que combina expertise externa, automação e inteligência artificial.

EXPERTOS EN CIBERSEGURIDAD LOGRARON BLOQUEAR MÁS DE 5 MIL ATAQUES BANCARIOS EN CHILE, Y OBSERVARON ADEMÁS, UN AUMENTO DE AMENAZAS DIRIGIDDAS SMARTPHONES

TrendTIC - De acuerdo con reciente informe realizado por empresa especializada en ciberseguridad, se han registrado 1,8 millones de ataques de troyanos bancarios bloqueados entre agosto de 2024 y junio de 2025 — un promedio de unos 5,000 por día. A pesar de la caída de casi la mitad (45,5%) respecto al año anterior (3,3 millones), el peligro no ha disminuido, solo se ha transformado. Para el caso de Chile se registraron más de 5 mil bloqueos. El informe señala un cambio en el enfoque de los ciberdelincuentes: los ataques están migrando de las computadoras a los dispositivos móviles, siguiendo el aumento del uso de los smartphones en transacciones financieras.

ARGENTINA DELINEA LINEAMIENTOS DE CIENCIA, TECNOLOGÍA E INNOVACIÓN PARA 2027

DPL News - El gobierno argentino oficializó la hoja de ruta de los próximos dos años de su Plan Nacional de Ciencia, Tecnología e Innovación 2030 (PNCTI2030). En la **Resolución 282/2025**, publicada por la Secretaría de Ciencia, Tecnología e Innovación (SICyT) contiene los lineamientos para el periodo 2025-2027. El documento prioriza promover cuatro sectores estratégicos: **Agroindustria, Energía y Minería, Economía del Conocimiento e Innovación** y **Salud**, por considerarlos “de alto impacto económico y social, con capacidad de generar empleo calificado, incrementar las exportaciones con valor agregado y fortalecer la competitividad internacional del país”.

POR PRIMERA VEZ EN UNA LEGISLATURA PROVINCIAL: SE REALIZA LA CUMBRE PARLAMENTARIA REGIONAL SOBRE IA Y CIBERSEGURIDAD

Legislatura Cordoba - Córdoba es la sede de la 3ª Cumbre Parlamentaria Regional “Forjando Futuros Digitales en el Cono Sur: IA, innovación, datos y ciberseguridad”, siendo la primera vez que esta reunión anual se realiza en una Legislatura provincial. Por este motivo, senadores, diputados y especialistas en tecnología, de países de América del Sur y Central, se reunieron en la Unicameral cordobesa para debatir sobre los desafíos y oportunidades que genera la transformación digital y la gobernanza de internet. De esta manera, entre lunes y martes, se realizarán mesas temáticas como “Innovación pública y transformación digital del Estado”; “Innovación, tecnología y sector privado — El rol de las empresas en la agenda de IA y desarrollo sostenible”; y “Tecnologías emergentes e innovación: oportunidades y riesgos”. El intercambio de experiencias será entre participantes que provienen de Argentina, Paraguay, Uruguay, Costa Rica, Panamá y México, entre otros.

US PROSECUTORS SAY CYBERSECURITY PROS RAN CYBERCRIME OPERATION

Reuters - Prosecutors said three American cybersecurity professionals secretly ran a ransomware operation aimed at shaking down companies across the United States. The three people, only two of whom - Ryan Goldberg and Kevin Martin - were identified by name, collaborated with the notorious hacking gang ALPHV BlackCat to encrypt companies' networks in a bid to extort their owners out of millions of dollars' worth of cryptocurrency, prosecutors alleged in an indictment filed last month, opens new tab in federal court in Miami.

HOW PETS HELP BANKS PROTECT CONSUMERS FROM FRAUD WITHOUT SHARING PERSONAL DATA

WEF - Fraud is rising, but collaboration between banks can reverse this trend. Privacy-enhancing technologies (PETs) let organizations derive insights together while keeping raw data under each party’s control. PETs enable banks to collaborate in ways that respect privacy and deliver the protection consumers expect. Fraud keeps climbing. In the United States alone, consumers reported more than $12.5 billion in losses in 2024, up about 25% year-over-year. Behind that figure are victims whose savings were drained, whose credit scores were destroyed by fraudulent loans, and whose stolen identities continue to cause harm long after the initial incident.

CYBERCRIMINALS EXPLOIT REMOTE MONITORING TOOLS TO INFILTRATE LOGISTICS AND FREIGHT NETWORKS

The Hacker News - Bad actors are increasingly training their sights on trucking and logistics companies with an aim to infect them with remote monitoring and management (RMM) software for financial gain and ultimately steal cargo freight. The threat cluster, believed to be active since at least June 2025 according to Proofpoint, is said to be collaborating with organized crime groups to break into entities in the surface transportation industry with the end goal of plundering physical goods. The most targeted commodities of the cyber-enabled heists are food and beverage products. "The stolen cargo most likely is sold online or shipped overseas," researchers Ole Villadsen and Selena Larson said in a report shared with The Hacker News. "In the observed campaigns, threat actors aim to infiltrate companies and use their fraudulent access to bid on real shipments of goods to ultimately steal them."