DIGI AMERICAS ALLIANCE MEMBERS

EL GOBIERNO LANZA UN NUEVO SISTEMA DE INTELIGENCIA - ARGENTINA

El Observador - El Gobierno tiene previsto lanzar en los próximos días un nuevo "sistema de inteligencia nacional" para integrar la información en sectores claves de la economía y en disputas internacionales una base para "mejorar el análisis estratégico", según aseguró a El Observador una fuente oficial vinculada al área. "Se establece una red de información de organismos estatales que aportará a la SIDE datos relevantes, aunque no produzcan inteligencia en el sentido estricto", explicó la fuente. Y aclaro que la ciberseguridad y protección de redes (cuya responsabilidad depende de la Secretaría de Innovación, dependiente de la Jefatura de Gabinete) será claramente distinguida de la ciberinteligencia, para "la obtención de conocimiento estratégico desde el ciberespacio para la toma de decisiones".

ANCI PUBLICA EN DIARIO OFICIAL SET DE NUEVOS INSTRUCTIVOS PARA OIV Y SERVICIOS ESENCIALES - CHILE

TrendTIC - La implementación de la Ley Marco de Ciberseguridad continúa avanzando con mayor precisión regulatoria. En ese contexto, la Agencia Nacional de Ciberseguridad (ANCI) oficializó un nuevo paquete de instrucciones generales que refuerzan tanto los aspectos operativos como de gobernanza que deberán cumplir las instituciones públicas y privadas que prestan servicios esenciales o que han sido calificadas como Operadores de Importancia Vital. Se trata de las Instrucciones Generales N°2, N°3 y N°4, publicadas en el Diario Oficial, que consolidan el tránsito desde un enfoque declarativo hacia uno plenamente ejecutable en materia de ciberseguridad.

NOVA NORMA DA ANATEL ELEVA A BARRA DE SEGURANÇA PARA FORNECEDORES DE TECNOLOGIA - BRASIL

InforChannel - Desde 26 de novembro, o setor de telecomunicações brasileiro ingressou em uma nova fase, com a entrada em vigor da obrigatoriedade de auditoria independente da Política de Segurança Cibernética (PSC) para todos os fornecedores de produtos e equipamentos de telecomunicações que atendem operadoras no País. Estabelecida pela Agência Nacional de Telecomunicações (Anatel) por meio do Ato nº 16.417, publicado em 26 de novembro de 2024, a medida institui um novo patamar de responsabilidade e rastreabilidade para os dispositivos que integram as redes de telecom no Brasil.

BRAZIL: BCB AND CMN ESTABLISH ADDITIONAL CYBER SECURITY REQUIREMENTS

Global Compliance News - On 18 December 2025, the Central Bank of Brazil (BCB) published National Monetary Council (CMN) Resolution No. 5,274/2025 and BCB Resolution No. 538/2025, both amending previous rules on cybersecurity and requirements for contracting cloud processing, storage and computing services for institutions regulated by the BCB. CMN Resolution No. 5,274/2025 amends CMN Resolution No. 4,893/2021, while BCB Resolution No. 538/2025 amends BCB Resolution No. 85/2021.

COLOMBIA SE ENCAMINA HACIA UNA CIBERSEGURIDAD PREDICTIVA IMPULSADA POR IA DE CARA A 2026

Prensario TI Latin America - La ciberseguridad en Colombia se prepara para un cambio estructural profundo. De acuerdo con el análisis de SISAP, compañía regional especializada en seguridad de la información, el país está ingresando en una nueva etapa en la que la protección digital dejará de ser mayoritariamente reactiva para convertirse en predictiva y autónoma, impulsada por inteligencia artificial (IA) y automatización avanzada. Durante 2025, las organizaciones enfocaron sus esfuerzos en mitigar amenazas como el phishing avanzado, la exposición de credenciales, la ingeniería social y los ataques a terceros. Sin embargo, el escenario hacia 2026 marcará un punto de quiebre definitivo. Los ciberdelincuentes ya están adoptando IA ofensiva, es decir, agentes autónomos capaces de analizar, decidir y ejecutar ataques sin intervención humana, lo que acelera los tiempos y eleva significativamente el nivel de sofisticación del crimen digital.

INVESTIGAN DAÑOS EN CABLE SUBMARINO DE TELECOMUNICACIONES EN EL GOLFO DE FINLANDIA

Cadena3 - Las autoridades investigan el daño causado a un cable de telecomunicaciones submarino en el Golfo de Finlandia que ocurrió el miércoles temprano entre las capitales de Finlandia y Estonia. Las autoridades finlandesas incautaron e inspeccionaron el buque sospechoso de haber causado el daño, informó la guardia fronteriza en un comunicado. Su ancla estaba bajada cuando fue descubierto en la zona económica exclusiva de Finlandia. La policía de Helsinki ha abierto una investigación por posible daño criminal agravado, intento de daño criminal agravado e interferencia agravada con las telecomunicaciones. El cable pertenece al proveedor de servicios de telecomunicaciones Elisa y se considera una infraestructura submarina crítica. El daño ocurrió en la zona económica exclusiva de Estonia, según la policía. Finlandia está preparada para desafíos de seguridad de diversos tipos, y respondemos a ellos según sea necesario, escribió el presidente finlandés Alexander Stubb en la plataforma social X. Las autoridades estonias están cooperando con las finlandesas para decidir si deben iniciar un caso penal separado o avanzar en una acusación conjunta.

CIBERSEGURIDAD Y EL TSUNAMI TECNOLÓGICO DE 2026: LA COLISIÓN ENTRE IA, LA COMPUTACIÓN CUÁNTICA Y LA WEB 4.0

Portal Innova - El año 2026 no se definirá por actualizaciones graduales. Estará marcado por una colisión de fuerzas sin precedentes: la informática de última generación, la hiperautomatización y un ajuste de cuentas global en materia de ciberseguridad. De acuerdo a Check Point Software Technologies, el panorama que se avecina se anticipa en las siguientes diez predicciones.

WHY RUSSIAN HACKERS ARE ABANDONING ZERO-DAYS FOR MISCONFIGURATIONS

Security Buzz - For years, elite state-backed hackers have been defined by their exploits. Zero-days were the calling card—rare bugs, complex chains, techniques that only a handful of teams could pull off. That image still dominates how many defenders think about top-tier threats. Amazon's latest threat intelligence challenges that assumption. According to AWS, Russian state-sponsored attackers tied to Sandworm are increasingly gaining access through misconfigured network edge devices, exposed management interfaces, and cloud environments with overly permissive settings. These attackers haven't lost the ability to exploit software; they've simply chosen not to. If misconfigurations get them in quietly and with little risk, there's no reason to burn a valuable exploit.

CARETO HACKER GROUP IS BACK AFTER 10 YEARS OF SILENCE WITH NEW ATTACK TACTICS

Cybersecurity News - After a decade of disappearing from the cybersecurity landscape, the Careto threat group, also known as "The Mask," has resurfaced with sophisticated new attack methods targeting high-profile organizations. Security researchers have identified fresh evidence of Careto's activity, revealing how the group evolved its tactics to compromise critical infrastructure and maintain persistent access to sensitive networks. The Careto group has been conducting advanced cyberattacks since at least 2007, traditionally focusing on government agencies, diplomatic entities, and research institutions. Careto aka The Mask resurfaces after a decade, launching advanced attacks on high-profile targets and critical infrastructure.

TELECOM OPERATORS' CYBERSECURITY SPENDING TO HIT $42B IN SIX YEARS

The Guardian - The Groupe Spéciale Mobile Association (GSMA) has warned that fragmented cybersecurity regulation is raising costs and increasing mobile operators' risk. GSMA, in a new independent study titled "The Impact of Cybersecurity Regulation on Mobile Operators," revealed that mobile operators are spending between $15-19 billion yearly on core cybersecurity activities, a figure expected to rise to $40-42 billion by 2030. Despite this significant investment, the telecom body said mobile network operators, which form the backbone of digital economies worldwide, are impacted by poorly designed, misaligned or overly prescriptive regulation, which results in unnecessary costs, diverting resources from genuine risk mitigation, and in some cases increasing exposure to cyber threats.

WHAT EVERY COMPANY NEEDS TO KNOW ABOUT CYBERSECURITY IN 2026

Forbes - 2026 is a pivotal juncture for cybersecurity. What was once considered an operational safety net and a business cost item is now a determinant of long-term competitiveness, market confidence, and organizational resilience. The data unequivocally indicates that cyber danger is systemic rather than episodic. The difficulty facing firms in 2026 is not whether to invest in cybersecurity, but rather how to integrate it with governance, corporate strategy, and operational continuity.