DIGI AMERICAS ALLIANCE MEMBERS

PARAGUAY OFICIALIZA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2025-2028

dpl news - El gobierno paraguayo publicó y oficializó la Estrategia Nacional de Ciberseguridad (ENC) para el periodo 2025-2028, que será implementada por el Ministerio de Tecnologías de la Información y Comunicación (Mitic), para fortalecer la seguridad digital del país. La aprobación de la iniciativa se da tras un proceso de poco más de un año, iniciado en marzo de 2024, que involucró al gobierno, el sector privado, la academia y la sociedad civil. La ENC actualiza el instrumento anterior, de 8 años de antigüedad, el Plan Nacional de Ciberseguridad 2017.

CIBERSEGURIDAD EN URUGUAY: EL PROGRESO QUE POCOS ESTÁN VIENDO

msn - En ese escenario regional, Uruguay aparece como uno de los países que supo adelantarse a la tendencia. "Uruguay hizo un muy buen trabajo", valoró Chain, quien destacó el rol de la Agencia de Gobierno Electrónico y Sociedad de la Información: "AGESIC hizo un trabajo enorme con todo lo que es la seguridad de la información". Aunque reconoce que el país aún enfrenta desafíos importantes, especialmente en lo que refiere a la educación digital de la población, Chain subraya que "fue durante un tiempo la prioridad, fue una de las prioridades esto de querer concientizar".

ANATEL APRESENTA AVANÇOS EM CONECTIVIDADE E SEGURANÇA DIGITAL EM REUNIÃO DO CONSELHO CONSULTIVO - BRASIL

gov.br - A Anatel apresentou, nesta terça-feira (20/5), os principais resultados e avanços regulatórios, tecnológicos e institucionais do ano de 2024 ao Conselho Consultivo da Agência, em reunião realizada em Brasília. A reunião, presidida por Fabrício da Mota Alves, teve como pauta central a apreciação do Relatório Anual de Gestão, elaborado sob coordenação da Superintendência Executiva, com participação e considerações do superintendente executivo, Gustavo Santana Borges, e apresentação técnica conduzida por Marcelo Monteiro, gerente de Planejamento Estratégico. Também esteve presente, na ocasião, o superintendente de Outorga e Recursos à Prestação, Vinicius Caram.

GOVERNO ANUNCIA GRUPO PARA ELABORAR PLANO NACIONAL DE CIBERSEGURANÇA - BRASIL

Olhar Digital - O Comitê Nacional de Cibersegurança (CNCiber) criará um grupo de trabalho temático para elaborar o Plano Nacional de Cibersegurança. O plano visa criar recomendações para o mercado de tecnologia e de prestadores de serviços digitais no que diz respeito à segurança cibernética no Brasil. A criação do grupo foi publicada em resolução desta terça-feira (27), no Diário Oficial da União (DOU). Ele contará com representantes do governo, mercado e sociedade civil.

CIBERSEGURANÇA NOS ESTADOS BRASILEIROS

BID - Em 2024, em parceria com o Subgrupo de Trabalho de Segurança Cibernética do GTD.GOV, o BID conduziu um mapeamento das configurações organizacionais relacionadas à segurança da informação e segurança cibernética nas 27 unidades federativas brasileiras. Essa pesquisa pioneira analisou a partir de questionários pré-estruturados políticas, modelos de governança e capital humano para os temas de cibersegurança. O relatório oferece a primeira visão do quebra-cabeça da governança da cibersegurança nos estados brasileiros.

PROTECCIÓN DE PAGOS DIGITALES EN COLOMBIA: 5 CLAVES PARA TRANSACCIONES SEGURAS

Revista C-Level - Con más de USD 13.500 millones en ventas proyectadas para 2027, el comercio electrónico en Colombia avanza a paso firme. Pero junto al auge de las transacciones digitales, también se multiplican los riesgos: suplantación de identidad, phishing, smishing, vishing, robo de dispositivos y clonación de sitios web. La protección de pagos digitales en Colombia se ha convertido en una prioridad.

INFRAESTRUCTURA INVISIBLE - COLOMBIA

El Universal - En la era digital, los centros de datos son tan importantes como los puertos y autopistas en el siglo XX. Constituyen la infraestructura invisible que hace posible desde las transferencias bancarias hasta la inteligencia artificial. Colombia está rezagada en esta infraestructura estratégica. Hoy, más del 80% de los datos que utilizamos se procesan fuera del país, principalmente en EE. UU. y Brasil. Esto genera mayor latencia, dependencia tecnológica, costos elevados y riesgos en materia de ciberseguridad. Un país que aspire a cobrar dividendos digitales no puede depender de la infraestructura ajena.

AVANZA EN ANÁLISIS DE INICIATIVA DE LEY DE CIBERSEGURIDAD - GUATEMALA

Congreso.gob.gt - Con el objetivo de avanzar con el análisis de la iniciativa 6347, ley de Ciberseguridad, la Comisión de Asuntos de Seguridad Nacional, presidida por el diputado Jorge Mario Villagrán, se reunió de manera híbrida con la mesa técnica de asesores, para abordador con el Título III, el cual aborda medidas cautelares, procesales y procedimentales. Participaron de forma virtual los diputados Felipe Alejos, José Pablo Mendoza, Rodrigo Pellecer y los congresistas Darwin Lucas, Mirna Godoy Palala estuvieron de manera presencial.

GUATEMALA Y EE. UU. ESTRECHAN LAZOS EN INNOVACIÓN TECNOLÓGICA

Republica - Es noticia. El embajador de EE. UU. en Guatemala, Tobin Bradley, recibió en su residencia a inversionistas de Silicon Valley interesados en explorar oportunidades en el sector tecnológico del país. Durante el encuentro, se discutieron posibles inversiones en áreas clave como inteligencia artificial, ciberseguridad y manejo de datos. Bradley enfatizó que el mundo de la tecnología se mueve rápido y que EE. UU. y Guatemala se mueven con él. Asimismo, subrayó la importancia de la colaboración bilateral para abrir nuevos mercados y fortalecer la seguridad y prosperidad de ambos países y la región.

CIBERATAQUES EN AMÉRICA LATINA: TENDENCIAS ALARMANTES Y ESTRATEGIAS DE DEFENSA EMERGENTES

Reporte Diario - El Índice de Inteligencia de Amenazas X-Force 2025 de IBM revela una imagen preocupante del panorama cibernético en América Latina. La región representó el 8% de todos los incidentes respondidos por X-Force en 2024, una disminución del 12% del año anterior, pero aún una cifra alarmante. Los ciberdelincuentes continúan adaptando sus tácticas, centrándose en métodos más sigilosos y rentables, como el robo de credenciales y el uso de infostealers.

NEW GUIDANCE FOR SIEM AND SOAR IMPLEMENTATION

CISA - Today, CISA, in collaboration with the Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC) and other international and U.S. partners, released new guidance for organizations seeking to procure Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms. This guidance includes the following three resources: Implementing SIEM and SOAR Platforms – Executive Guidance outlines how executives can enhance their organization’s cybersecurity framework by implementing these technologies to improve visibility into network activities, enabling swift detection and response to cyber threats. Implementing SIEM and SOAR Platforms – Practitioner Guidance focuses on how practitioners can quickly identify and respond to potential cybersecurity threats and leverage these technologies to streamline incident response processes by automating predefined actions based on detected anomalies. Priority Logs for SIEM Ingestion – Practitioner Guidance offers insights for prioritizing log ingestion into a SIEM, ensuring that critical data sources are effectively collected and analyzed to enhance threat detection and incident response capabilities tailored for organizations.

THE DOUBLE-EDGED SWORD OF CYBERSECURITY INNOVATIONS

JPMorgan - In an era defined by accelerating cyberthreats and technological disruption, founders face a complex, evolving landscape. Regardless of industry, this is a reality for startups, whether they’re developing a first prototype, fine-tuning a go-to-market strategy or preparing to go public. The same advances in artificial intelligence (AI), cloud computing and automation that enhance companies’ defenses are simultaneously exploited by adversaries. On the horizon, quantum computing promises to reshape encryption and cryptanalysis, making data protection and offensive capabilities more powerful.

STATE OF HEALTHCARE CYBERSECURITY: PROGRESS AND PITFALLS

Govinfosecurity - While the healthcare sector is making progress in cyber resilience, it still faces deep-rooted challenges, including collaboration, cyber workforce issues and budget constraints, necessitating a constant demand for adaptation and re-prioritization as adversaries shift their tactics, said security experts Phil Englert and Murad Dikeidek. Information sharing can be vital to helping the overall sector better understand the threats it is facing, yet there's still uncertainty at many organization about the level of details healthcare providers should disclose, he said.

WHY AI IS THE NEW CYBERSECURITY BATTLEGROUND

Forbes - Artificial intelligence has quickly grown from a capability to an architecture. As models evolve from backend add-ons to the central engine of modern applications, security leaders are facing a new kind of battlefield. The objective not simply about protecting data or infrastructure—it’s about securing the intelligence itself. In this new approach, AI models don’t just inform decisions—they are decision-makers. They interpret, respond, and sometimes act autonomously. That shift demands a fundamental rethink of how we define risk, build trust, and defend digital systems.