DIGI AMERICAS LATAM CISO

INSIGHTS

OCTOBER 16, 2025

DIGI AMERICAS ALLIANCE MEMBERS

PLAN CONECTA: INSTITUCIONES FORTALECEN LA CIBERSEGURIDAD Y DEFENSA CIBERNÉTICA - GUATEMALA

AGN - Ciudad de Guatemala, 14 oct (AGN).- Proteger la información del país es una prioridad estratégica del Plan Conecta, liderado por el Ministerio de Comunicaciones, Infraestructura y Vivienda (CIV), que busca fortalecer la conectividad y la transformación digital del país. En este sentido, el CIV, a través de la Superintendencia de Telecomunicaciones (SIT), desarrolló la jornada de capacitación Evaluación Nacional CIRT de Guatemala Versión 1.0, enfocada en fortalecer la seguridad cibernética nacional y preparar al país ante amenazas digitales.

ANATEL QUER DATA CENTERS FORA DO SUDESTE E REFORÇA REGULAÇÃO - BRASIL

Convergencia Digital - A Anatel defende a desconcentração dos data centers instalados no Sudeste e a expansão dessa infraestrutura essencial para outras regiões do país, como forma de reduzir riscos, melhorar a conectividade e fortalecer a soberania digital brasileira. A recomendação faz parte do White Paper Data Centers no Brasil, que reúne diagnósticos técnicos e propostas regulatórias para o setor. O estudo reconhece que os data centers — instalações que armazenam e processam dados — são hoje infraestruturas críticas da economia digital, sustentando desde serviços públicos até operações bancárias, sistemas de saúde e plataformas de telecomunicações.

SEGURANÇA CIBERNÉTICA EM FINTECHS GANHA URGÊNCIA DIANTE DO AVANÇO DAS AMEAÇAS DIGITAIS - BRASIL

Economic News Brasil - A segurança cibernética em fintechs passou a ser prioridade para reguladores e empresas após uma série de falhas recentes, incluindo o episódio do fintech Monbank, em setembro de 2025, que expôs dados de clientes e gerou alerta para todo o sistema financeiro. O caso, em que um ataque hacker desviou R$ 4,9 milhões do banco digital, revelou que mesmo instituições em conformidade com as regras básicas podem sofrer incidentes quando não há monitoramento contínuo de vulnerabilidades.

DIGI AMERICAS LATAM CISO

INSIGHTS

OCTOBER 16, 2025

SÁNCHEZ ANUNCIA LA CREACIÓN DE UN NUEVO CENTRO NACIONAL DE CIBERSEGURIDAD - ESPAÑA

Publico - El presidente del Gobierno, Pedro Sánchez, ha anunciado este jueves la próxima creación de un Centro Nacional de Ciberseguridad. Este organismo estará adscrito a la Presidencia del Gobierno, según ha destacado el propio Sánchez durante el acto de clausura de la 19ª edición del Encuentro Internacional de Seguridad de la Información (ENISE), organizado por el Instituto Nacional de Ciberseguridad de España (INCIBE), en León. El objetivo de esta iniciativa es "reforzar la coordinación y la fortaleza" del sistema nacional de ciberseguridad. Se unirá a la revisión ya puesta en marcha de la Estrategia Nacional de Ciberseguridad del Plan España Digital. El presidente del Gobierno ha destacado tres ejes de actuación en esta materia. Por un lado, fortalecer el ecosistema de la ciberseguridad en nuestro país. Por otro, "fomentar la innovación" y, por último "aumentar la inversión".

EL CCN ESPAÑOL REFUERZA LA CIBERSEGURIDAD EN LATINOAMÉRICA CON UNA FORMACIÓN DIRIGIDA A 18 PAÍSES

Segurilatam - El Centro Criptológico Nacional (CCN) de España ha puesto en marcha la tercera edición del programa de formación de ciberseguridad «Ruta Esencial de Gestión de Incidentes», dirigido los equipos de respuesta a incidentes de 18 países de Iberoamérica. Durante 28 semanas, cerca de cien especialistas en ciberseguridad pertenecientes a la Red CSIRTAmericas recibirán formación técnica avanzada a través de la Ángeles, la plataforma de formación, capacitación y talento en ciberseguridad del CCN.

RANSOMWARE Y ESPIONAJE INDUSTRIAL: LOS DESAFÍOS CRÍTICOS DEL SECTOR MANUFACTURERO - CHILE

TrendTIC - La industria de la manufactura enfrenta un conjunto de riesgos complejos que operan con mínima tolerancia al tiempo de inactividad, además forman parte de cadenas de suministro extensas y muchas veces complejas, y su ventaja competitiva generalmente se basa en propiedad intelectual de alto valor, como diseños patentados y secretos comerciales. Los equipos responsables de IT y seguridad, necesitan estar en alerta, ya que los ciberataques modernos son sofisticados y persistentes al combinar exploits técnicos con ingeniería social y robo de credenciales; debido a que buscan pasar desapercibidos, recopilando información y mapeando sistemas antes de atacar.

BOTS Y DEEPFAKES IMPULSAN UNA NUEVA OLA DE FRAUDES CIBERNÉTICOS: LA SUMA IMPORTANCIA QUE TIENE PARA LAS COMPAÑÍAS DE CIBERSEGURIDAD COMUNICAR EN SITIOS OFICIALES, DE NICHO, PRESTIGIO E INDEPENDIENTES - CHILE

TrendTIC - Internet está entrando en una nueva era de sofisticación, y lo mismo ocurre con las estafas en línea. Desde familiares clonados con IA que piden dinero hasta ejecutivos deepfake que engañan a empleados para realizar transferencias millonarias, el fraude en línea ha evolucionado desde enlaces de phishing hasta identidades sintéticas que se ven y suenan reales. Solo este año, el fraude mediante deepfakes podría aumentar un 162%, afectando tanto a empresas como a personas.

DIGI AMERICAS LATAM CISO

INSIGHTS

OCTOBER 16, 2025

LA PROTECCIÓN DE LAS INFANCIAS EN INTERNET COMO ELEMENTO DE SOBERANÍA DIGITAL

DPL News - El debate sobre la regulación digital ha dejado de ser un asunto meramente técnico para convertirse en un eje central de las discusiones políticas, económicas y geopolíticas a nivel global. La reciente intervención del presidente de Brasil, Luiz Inácio Lula da Silva, ante la ONU lo demuestra con claridad: proteger a los más vulnerables en el entorno digital, especialmente a niños y adolescentes, no es sólo una cuestión de derechos humanos, sino también un imperativo democrático y estratégico. En un contexto donde Internet ha amplificado tanto las oportunidades como los riesgos, el establecimiento de marcos normativos se vuelve necesario, aunque requiere diálogo y consenso.

OFFICIALS CRACK DOWN ON SOUTHEAST ASIA CYBERCRIME NETWORKS, SEIZE $15B

Cyberscoop - Federal authorities seized 127,271 Bitcoin, valued at approximately $15 billion, from Chen Zhi, the alleged leader of a sprawling cybercrime network based in Cambodia, the Justice Department said Tuesday. Officials said it's the largest financial seizure on record. Officials said Chen, a 38-year-old United Kingdom and Cambodian national who has renounced his Chinese citizenship, built a business empire under the Prince Group umbrella headquartered in Phnom Penh, Cambodia, that constructs, operates and manages scam compounds that rely on human trafficking and modern-day slavery.

CYBERCRIMINALS IMPERSONATE OPENAI AND SORA TO HARVEST USER CREDENTIALS

Cyber Press - The launch of Sora 2 AI has triggered a surge in malicious activity, as cybercriminals deploy deceptive domains impersonating OpenAI's official services to steal user credentials and conduct large-scale crypto fraud. Multiple threat intelligence reports confirm that cloned Sora webpages are being used for credential harvesting, crypto wallet theft, and unauthorized access to paid API plans.

CYBERSECURITY AND OTHER CRITICAL ISSUES TAKE CENTRE STAGE AS EXPERTS MEET IN DUBAI

WEF - Hundreds of experts on a wide range of critical topics converged on Dubai, United Arab Emirates, this week for the World Economic Forum's Annual Meetings of the Global Future Councils and Cybersecurity (AMGFCC). The joint gathering between the Annual Meeting of the Global Future Councils (AMGFC) and the Annual Meeting on Cybersecurity (AMC) took place against a backdrop of jarring geopolitical shifts and advances in artificial intelligence, a hardening of multipolarity, and increased vulnerability to cyber threats and disinformation.