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

MÉXICO Y REPÚBLICA DE ESTONIA BUSCARÁN EL INTERCAMBIO EN MATERIA DE DIGITALIZACIÓN GUBERNAMENTAL Y CIBERSEGURIDAD

Talla Politica - Al instalarse el Grupo de Amistad México-República de Estonia, su presidenta la diputada Deliamaria González Flandez (PVEM) mencionó que este tendrá como propósito el intercambio en materia de digitalización gubernamental, ciberseguridad, capacitación tecnológica y el comercio electrónico. La legisladora indicó que la relación de ambas naciones se basa en los valores compartidos y en una visión común al futuro. “México como nación diversa y con un papel estratégico en la región y Estonia como una potencia en la digitalización, gobierno electrónico e innovación han construido un diálogo binacional que se fundamenta en el respeto y la cooperación”.

REPÚBLICA DOMINICANA ASUME LA PRESIDENCIA 2026 DE LA RED GEALC

Presidencia.gob.do - La República Dominicana fue elegida para integrar el Comité Ejecutivo y asume la Presidencia 2026 de la Red Interamericana de Gobierno Digital (Red GEALC). El anuncio se realizó durante la XIX Reunión Anual de la Red GEALC, celebrada en Guatemala, donde la Oficina Gubernamental de Tecnologías de la Información y Comunicación (Ogtic) representó al país.Reyson Lizardo, director de Transformación Digital Gubernamental de la Ogtic, así expresó desde allí: “Este logro reafirma el compromiso de la República Dominicana con la innovación, la transparencia y la eficiencia del Estado, y consolida nuestro papel como referente en gobierno digital en América Latina y el Caribe”.

EXTORSIONES EN SALUD SE TRIPLICAN Y 88 GRUPOS DE CIBERDELINCUENTES AMENAZAN AL SECTOR - CHILE

TrendTIC - El sector salud enfrenta una nueva fase de riesgo en materia de ciberseguridad. De acuerdo con el informe sobre el «Estado del Ransomware en el sector sanitario 2025» realizado por expertos en ciberseguridad, la extorsión basada únicamente en robo de datos -sin necesidad de cifrarlos o bloquearlos- se triplicó desde 2023, convirtiéndose en la modalidad de ciberataque más agresiva y con mayor crecimiento entre todos los sectores económicos analizados en el estudio.

LULA DA SILVA CRITICA EN EL G20 LA CONCENTRACIÓN TECNOLÓGICA Y PIDE GOBERNANZA DE LA IA - BRASIL

DPL News - Durante su discurso en la Cumbre del G20, en Johannesburgo, el presidente de Brasil, Luiz Inácio Lula da Silva, volvió a criticar la concentración global de tecnología y defendió una mayor autonomía digital para los países en desarrollo. El mandatario afirmó que el control de datos, algoritmos e infraestructura por parte de las grandes economías profundiza las desigualdades y puede configurar un “colonialismo digital”.

TENDÊNCIAS PARA O MERCADO DE SEGURANÇA ELETRÔNICA NO BRASIL EM 2026

Revista Seguranca Eletronica - O mercado de segurança eletrônica no Brasil consolida-se como um dos mais dinâmicos da América Latina, projetado para alcançar um faturamento superior a R$ 18 bilhões em 2026, impulsionado por um crescimento anual composto (CAGR) de cerca de 12% a partir dos R$ 14 bilhões registrados em 2024.

EL FORO IBEROAMERICANO DE CIBERDEFENSA SE REÚNE EN MADRID

Segurilatam - Madrid acogió, el 26 de noviembre, la VIII edición del **Foro Iberoamericano de Ciberdefensa**. España, al ser la titular de la Secretaría Pro-Témpore, fue la sede de este encuentro coincidiendo con la celebración de las Jornadas STIC organizadas por el Centro Criptológico Nacional y el **Mando Conjunto del Ciberespacio** españoles. El general de división Gómez Lera presidió la que fue la primera reunión presencial del Foro.

ADAPTARSE AL CONSUMIDOR, EL PASO CLAVE PARA DIGITALIZAR A LAS PYMES DE LA REGIÓN

Revista E&N - ¿Cómo ayudar a las pymes para que den un salto en la transformación digital? Desde Miami, el Mastercard Innovation Forum propone una hoja de ruta paras las pequeñas y medianas empresas de la región, protagonistas del 75% del empleo global. Si bien no hay una solución única debido a la particularidad de cada empresa, la propuesta es que las PYMES se adapten a los hábitos de consumo de sus clientes y adopten todo tipo de portafolio de pagos digitales. La idea es acompañar a los dueños de negocios en la construcción, crecimiento y protección de sus empresas en una economía cada vez más digital.

ALMOST 1 BILLION ATTEMPTS TO ACCESS MALICIOUS SITES BLOCKED BY NEW GOVERNMENT CYBER TOOL - UNITED KINGDOM

NCSC - Almost one billion early-stage cyber attacks and attempts to access scam websites have been blocked by a new government cyber service in less than a year, according to new figures from GCHQ’s National Cyber Security Centre (NCSC) and BT. The Share and Defend service – developed by experts at NCSC – works to disrupt online crime by sharing near real-time data on known fraudulent and malicious websites with internet service providers, which can then prevent customers from clicking through.

NSA, CISA, AND OTHERS RELEASE GUIDANCE ON INTEGRATING AI IN OPERATIONAL TECHNOLOGY - USA

NSA - The National Security Agency (NSA) is joining the Cybersecurity and Infrastructure Security Agency (CISA), the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), and others in releasing the Cybersecurity Information Sheet (CSI), "Principles for the Secure Integration of Artificial Intelligence in Operational Technology." While artificial intelligence (AI) presents potential to enhance efficiency, productivity, decision-making, and customer experiences, adopting AI into operational technology (OT) systems introduces new risks to the safety and security of the environments they are integrated in and critical functions they support.

AISURU BOTNET BEHIND NEW RECORD-BREAKING 29.7 TBPS DDOS ATTACK

Bleeping Computer - In just three months, the massive Aisuru botnet launched more than 1,300 distributed denial-of-service attacks, one of them setting a new record with a peak at 29.7 terabits per second. Aisuru is a huge botnet-for-hire service that provides an army of routers and IoT devices compromised via known vulnerabilities or through brute-forcing weak credentials. Internet management and infrastructure company Cloudflare estimates that the botnet uses between one and four million infected hosts across the world.

A DECADE OF RANSOMWARE CHAOS – HOW MUCH IT COSTS

Cybersecurity Ventures - IoT for all reports that over the past decade, ransomware has evolved from a small-scale threat targeting personal computers into a systemic risk affecting critical infrastructure, smart factories, and connected devices. In 2015, the FBI received approximately 2,400 ransomware complaints, resulting in losses exceeding $24 million. That same year, broader estimates put ransomware damage at around $300 million. By 2017, the scale had expanded, and damage estimates had risen to $5 billion. Fast forward to 2021, ransomware damages to organizations were estimated at $20 billion, according to Cybersecurity Ventures, with attacks occurring roughly every 11 seconds.

FIGHTING CYBER-ENABLED FRAUD: A SYSTEMIC DEFENCE APPROACH

WEF - Phishing and cyber-enabled fraud are escalating global threats affecting users, consumers, organizations and countries alike. This white paper, Fighting Cyber-Enabled Fraud: A Systemic Defence Approach, developed by the World Economic Forum's Partnership against Cybercrime in collaboration with the Institute for Security and Technology, presents a systemic defence framework to confront this challenge. Turning the tide on cyber-enabled fraud demands a truly systemic approach, one that maximizes the impact of upstream interventions while ensuring broad, consistent coverage through downstream measures, and this paper calls on stakeholders to act across three complementary pillars of systemic defence: Prevention, Protection and Mitigation. It also demonstrates how a multistakeholder, upstream-focused model can shift responsibility to those best positioned to act at scale, empowering them to prevent harm before it takes root.