DIGI AMERICAS ALLIANCE MEMBERS

MINISTERIO TIC LANZÓ EL PROGRAMA CIBERPAZ QUE LE APUESTA A UN INTERNET SEGURO, RESPETUOSO E INCLUYENTE - COLOMBIA

MINTIC - Desde la capital del Atlántico, en la Universidad Autónoma del Caribe y bajo el eslogan "El Caribe se conecta con CiberPaz", el Gobierno Nacional presentó el programa CiberPaz, que llegará a todo el país, en búsqueda de la promoción del uso consciente, empático, incluyente y responsable de las Tecnologías de la Información y las Comunicaciones, asegurando la participación de los colombianos en la era digital. "CiberPaz nos va a permitir llegar a esa Colombia profunda, a aquellos que no tienen voz, a aquellos que no aparecen en los grandes medios de comunicación ni en las grandes cadenas de televisión. También nos va a permitir construir territorio desde las mismas comunidades", destacó Belfor García, Viceministro de Transformación Digital del Ministerio TIC.

CNMP INSTITUI A POLÍTICA E O SISTEMA NACIONAL DE CIBERSEGURANÇA DO MINISTÉRIO PÚBLICO - BRASIL

CNMP - O Conselho Nacional do Ministério Público publicou, nesta quarta-feira, 3 de julho, a Resolução CNMP nº 294/2024, que institui a Política e o Sistema Nacional de Cibersegurança do Ministério Público (PNCiber-MP). O texto, aprovado por unanimidade em 28 de maio, durante a 8ª Sessão Ordinária de 2024, foi apresentado pelo corregedor nacional do Ministério Público, Ângelo Fabiano Farias, e relatado pelo então conselheiro Jayme de Oliveira. A resolução é composta por nove capítulos, que tratam das disposições gerais, dos princípios, dos objetivos, dos instrumentos, da governança e da gestão da PNCiber-MP, do Sistema Nacional de Cibersegurança, da cibersegurança nas unidades e ramos e da estratégia, do plano nacional de cibersegurança do MP e das disposições finais.

CIBERSEGURIDAD, PRIORIDAD DE LA BANCA MEXICANA; VIENEN INVERSIONES

Excelsior - Los bancos invertirán alrededor de 24 mil millones de pesos en ciberseguridad y el incremento de la oferta digital durante este año, de acuerdo con la Asociación de Bancos de México (ABM). Julio Carranza, líder de los banqueros, destacó que el año pasado se destinó esta misma cantidad a la protección contra los ciberdelincuentes y la ampliación de productos digitales derivado de la acelerada adopción de servicios financieros por internet. En su opinión el nivel de inversión debe dar certeza a los usuarios de la banca de que las instituciones financieras están comprometidas a no sufrir ciberataques que comprometan sus operaciones. Así como a ofrecer una oferta completa de servicios vía internet.

URUGUAY FORTALECERÁ SERVICIOS GUBERNAMENTALES DIGITALES CON APOYO DEL BID

BNAmericas - El Banco Interamericano de Desarrollo (BID) aprobó una Línea de Crédito Condicional para Proyectos de Inversión de US$74 millones para aumentar la eficiencia de la gestión pública, incrementar el nivel de seguridad del espacio digital y mejorar la gestión del sistema de salud de Uruguay a través del fortalecimiento de los servicios gubernamentales digitales. Esta Línea de Crédito para implementar el “Programa de Transformación Digital para un País Inteligente” incluye un primer préstamo individual de US$20 millones. Aunque Uruguay tiene un nivel muy alto de desarrollo del gobierno digital, existe la oportunidad de fortalecer los servicios gubernamentales en línea, especialmente en el sector salud, y de incrementar la capacidad detección y respuesta a incidentes en el ciberespacio dado el creciente número de ciberamenazas a nivel global.

FUERZAS MILITARES ESTÁN EN PLENO PROCESO DE FORTALECIMIENTO DE LA CIBERSEGURIDAD - PARAGUAY

LaNacion - Tras el anuncio realizado por el embajador itinerante de los Estados Unidos para el Ciberespacio y Política Digital, Nathaniel Fick sobre la cooperación de USD 3,1 millones para las Fuerzas Armadas, el ministro de Defensa Óscar González indicó que esto está en pleno desarrollo y que gracias a este proceso de fortalecimiento, ya se pudieron evitar hackeos. “El destacamento de Tecnología de las Fuerzas Militares fue el que alertó en una oportunidad hace unos meses sobre un intento o inicio de un hackeo a instituciones civiles, esta dependencia fue la que dio alerta en ese momento y gracias a eso se pudo subsanar rápidamente. Fue una intervención muy positiva de la dirección respectiva de las Fuerzas Militares y nosotros estamos en pleno proceso de fortalecimiento de esa área”, manifestó el secretario de Estado.

EXPERTOS PLANTEAN DEBATE SOBRE LA SEGURIDAD ANTE MAYOR BANCA DIGITAL - PARAGUAY

ÚltimaHora - En los últimos años, Paraguay ha experimentado un crecimiento exponencial en la adopción de la banca digital. Si bien esta tendencia ha facilitado el acceso a los servicios financieros y ha mejorado la inclusión financiera, también ha evidenciado la necesidad de garantizar la seguridad de las transacciones realizadas a través de estos canales. En ese sentido, el aumento de fraudes bancarios como vaciamientos de cuentas, SIM swapping y phishing ha generado preocupación entre los clientes y las autoridades. Al respecto, el analista y experto legal Stan Canova señala que la banca digital se expande a pasos agigantados, mientras que otros actores que deben acompañar este proceso en nuestro país están avanzando con un ritmo más cansino.

MINISTERIO DE DEFENSA CAPACITARÁ A PERSONAL DE LAS FUERZAS ARMADAS EN CIBERSEGURIDAD - PERÚ

Gob:pe - El Ministerio de Defensa capacitará a todo el personal del sector, personal militar en actividad, en retiro, licenciado y tropa de las Fuerzas Armadas en el “Programa Cibersoldados: Ciudadanos digitales capacitados y empoderados en la ruta de ciberseguridad”, que fue lanzado hoy en la sede institucional del sector. El evento fue liderado por el viceministro de Políticas para la Defensa, César Torres Vega, en representación del ministro Walter Astudillo Chávez, en presencia de la secretaria general, María Chumbe Rodríguez; el jefe de la Oficina General de Tecnología y de la Información y Estadística (OGTIE), Ernesto Castillo, así como representantes de las empresas aliadas.

ESTUDIO EN CIBERSEGURIDAD: CLAVES PARA FORTALECER EL DESARROLLO DIGITAL EN CHILE

ReporteMinero - Fortalecer el desarrollo digital de Chile, identificando áreas de mejora para avanzar en la seguridad de la información de las instituciones y personas, fue el objetivo que impulsó el desarrollo del estudio "Investigación y Desarrollo en Ciberseguridad", mandatado por el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación (MinCiencia). Para la Subsecretaria del MinCiencia, Carolina Gainza, la ciberseguridad es una prioridad estratégica. "La ciberseguridad es un tema de nuestro presente, que nos presenta desafíos y amenazas. Es esencial que trabajemos juntos para fortalecer nuestras capacidades y desarrollar soluciones innovadoras que respondan a estos desafíos".

70% DE ORGANIZACIONES NACIONALES NO TIENE PRESUPUESTO ADECUADO PARA CIBERSEGURIDAD - COSTA RICA

CRHoy - Un 70% de las organizaciones costarricenses encuestadas en un estudio académico afirma que el presupuesto que le asignan no es adecuado a las necesidades actuales en materia de ciberseguridad. Así se desprende del Estado de la Ciberseguridad en Costa Rica 2023, elaborado por el Laboratorio de Investigación, Desarrollo e Innovación en Ciberseguridad (LabCIBE) de la Universidad Nacional (UNA), cuyos resultados se obtuvieron por medio de una encuesta. A fin de recopilar información sobre el presupuesto asignado y los recursos disponibles con los que dispone la empresa para abordar temas de ciberseguridad en la infraestructura de su organización, se asignó una sección específica en la investigación, ya que la inversión en ciberseguridad se puede traducir como medidas preventivas, sistemas de detección e inclusive capacidad de respuesta, así como programas de formación y capacitación.

CIBERSEGURIDAD EN LATINOAMÉRICA ALCANZARÁ LOS USD$1,708 MILLONES

Mercado - El mercado de servicios de ciberseguridad gerenciada en América Latina está experimentando un crecimiento significativo. Según un informe de Frost & Sullivan, se espera que el mercado alcance los USD 1,708 millones para el año 2024, lo que representa un crecimiento del 12.8 % respecto al año 2023. Cabe señalar que la ciberseguridad gerenciada es un conjunto de soluciones que ofrece una empresa externa especializada a otra para gestionar su seguridad digital. En ese contexto, uno de los principales impulsores de este crecimiento es la falta de personal calificado.

NEW TAX ALLOWANCE TO BOLSTER CYBER SECURITY - T&T

Newsday - In a significant move to enhance the cyber security framework of TT, the National Information and Communication Technology Company Ltd (iGovTT), under the Digital Transformation Ministry, launched the Cybersecurity Investment Tax Allowance (CITA) management system on June 12. This initiative, part of the broader Cybersecurity Tax Administrative System (CySTAMS), was originally announced by Finance Minister in the 2023/2024 national budget. According to iGovTT, the platform allows businesses to submit proof of their cyber security purchases for validation, enabling them to claim tax credits up to $500,000 from the Inland Revenue Division of the Ministry of Finance.

MEKOTIO BANKING TROJAN THREATENS FINANCIAL SYSTEMS IN LATIN AMERICA

TrendMicro - The Mekotio banking trojan is a sophisticated piece of malware that has been active since at least 2015, primarily targeting Latin American countries with the goal of stealing sensitive information — particularly banking credentials — from its targets. Originating in the Latin American region, it has been particularly prolific in Brazil, Chile, Mexico, Spain, and Peru. Furthermore, Mekotio seems to share a common origin with other notable Latin American banking malware such as Grandoreiro, which was disrupted by law enforcement earlier this year. Mekotio is often delivered through phishing emails, employing social engineering to trick users into interacting with malicious links or attachments.

OPERATION REGULATION: STRENGTHENING LATIN AMERICA'S AI GOVERNANCE

ECFR - Recent elections in Latin America have underscored the dangerous impact of algorithms and AI, particularly generative AI, at the voting booth. During the 2023 Colombian regional election, campaigns were marred with misinformation funnelled across social media, with the emergence of AI-generated media content – or deepfakes – aimed at undermining candidates' political campaigns. This raised alarm bells among fact-checking groups like ColombiaCheck, as the widespread and convincingly realistic recordings enabled by generative AI's mimicry proved too difficult and time consuming to debunk before some damage was already done. A similar hoax sprung up during Argentina's 2023 election, where candidate Patricia Bullrich was the target of AI-generated audios slandering her minister of economy. In the recent Mexican election, a deepfake audio of candidate Claudia Sheinbaum mimicked her criticising President Andrés Manuel López and acknowledging fraud in the polls.

UNVEILING SUSPICIOUS PHISHING ATTACKS: ENHANCING DETECTION WITH AN OPTIMAL FEATURE VECTORIZATION ALGORITHM AND SUPERVISED MACHINE LEARNING

Frontiers - The dynamic and sophisticated nature of phishing attacks, coupled with the relatively weak anti-phishing tools, has made phishing detection a pressing challenge. In light of this, new gaps have emerged in phishing detection, including the challenges and pitfalls of existing phishing detection techniques. To bridge these gaps, this study aims to develop a more robust, effective, sophisticated, and reliable solution for phishing detection through the optimal feature vectorization algorithm (OFVA) and supervised machine learning (SML) classifiers.

HOW NATIONS CAN BUILD SOVEREIGN AI AND HOMEGROWN TALENT FOR ECONOMIC COMPETITIVENESS

WEF - Artificial intelligence is intellectually driven, not policy driven. It's about the people, and these are the people that build the foundation of what makes an AI ecosystem. The tech and algorithms in AI have been commoditized, but AI ecosystems become fully functioning when every stakeholder is aligned towards building the next generation of AI talent to populate their local ecosystems. Examples can already be seen across the United States. In December 2023, the state of New Jersey, NJEDA and Princeton University launched the NJ AI Hub for AI innovation and, a month later, the state of New York launched Empire AI, a state-of-the-art computing centre for ethical artificial intelligence (AI) research in collaboration with New York University, Columbia University and five other institutions.

HOW COMPANIES CAN MITIGATE AI'S GROWING ENVIRONMENTAL FOOTPRINT

HBR - By 2026, computing power dedicated to training AI is expected to increase tenfold. As more power is expended, more resources are needed. As a result, we've seen exponential increases in energy and perhaps more unexpectedly, water consumption. Some estimates even show running a large AI model generates more emissions over its lifetime than the average car. A recent report from Goldman Sachs found that by 2030, there will be a 160% increase in demand for power propelled by AI applications.

NOW THE EU COUNCIL SHOULD FINALLY UNDERSTAND: NO ONE WANTS "CHAT CONTROL"

EFF - The EU Council has now passed a 4th term without passing its controversial message-scanning proposal. The just-concluded Belgian Presidency failed to broker a deal that would push forward this regulation, which has now been debated in the EU for more than two years. For all those who have reached out to sign the "Don't Scan Me" petition, thank you—your voice is being heard. News reports indicate the sponsors of this flawed proposal withdrew it because they couldn't get a majority of member states to support it.