

DIGI AMERICAS ALLIANCE MEMBERS



SEGURANÇA CIBERNÉTICA EM DISCUSSÃO: DEBATE APONTA RISCOS DE ATAQUES E DESAFIOS PARA O BRASIL

Senado - Os prejuízos são contabilizados em mais de US\$ 10 trilhões. No Brasil, no planeta, os piratas da internet estão à solta em busca de alvos fáceis para a manipulação de dados. O Senado possui uma Subcomissão Permanente de Defesa Cibernética. E o programa Em Discussão desta semana traz o debate realizado sobre o tema. A audiência pública reuniu especialistas do setor.

NUCLEP RECEBE ABIN E AVANÇA EM PROTEÇÃO CIBERNÉTICA E DEFESA NACIONAL - BRASIL

Defesa em Foco - Nesta segunda-feira (23), a NUCLEP deu um passo significativo para aprimorar sua segurança cibernética e proteção de dados ao receber representantes da Agência Brasileira de Inteligência (ABIN). Em uma visita marcada pela troca de informações estratégicas, o presidente da NUCLEP, Carlos Henrique Silva Seixas, destacou a importância da colaboração para reforçar a defesa do setor nuclear e industrial do Brasil. O encontro também abriu novas possibilidades de parcerias entre as instituições, crucial para a proteção de tecnologias sensíveis.

EMBRATEL REFORÇA FOCO EM CIBERSEGURANÇA PARA O SETOR PÚBLICO - BRASIL

Tele Síntese - Com o aumento das ameaças digitais e a crescente necessidade de proteção de dados no setor público, a Embratel intensificou seus investimentos em cibersegurança e infraestrutura tecnológica. Em 2023, a empresa direcionou R\$ 9 bilhões para expandir sua rede e desenvolver novas soluções para seus clientes, principalmente para governos e prefeituras. No Inovatic 2024, promovido pelo Tele.Síntese, Ana Lucia Domiquili, diretora de vendas para governo da Embratel, afirmou que a empresa está focada em fornecer serviços que vão além da conectividade. Apresentando, assim, uma oferta que inclui cloud, IoT e data insights.

NATEL DETERMINA MEDIDAS DE COMBATE A FRAUDES E GOLPES TELEFÔNICOS - BRASIL

Agência Brasil - A Agência Nacional de Telecomunicações (Anatel) determinou nesta segunda-feira (23) um conjunto de medidas às prestadoras de serviços de telecomunicações com o objetivo de impedir o uso de ligações telefônicas para aplicação de golpes e fraudes. A agência reguladora esclarece que as medidas determinadas pretendem garantir a transparência e a rastreabilidade das ligações telefônicas e correspondem a uma resposta à atualização de métodos usados por fraudadores e ações complementares a outras disposições já implementadas pela Anatel e em andamento.

EXPERTOS EN CIBERSEGURIDAD SE REÚNEN EN PERÚ PARA FRENAR CIBERATAQUES EN LA REGIÓN

Andina - En el marco del Cyberdrill Regional para las Américas, un evento que busca reforzar la ciberseguridad en la región, y que se viene realizando en nuestro país con expertos nacionales e internacionales, hoy se dio inicio a los ejercicios de simulaciones de ciberataques y respuestas. Para este inicio, los técnicos de la Unión Internacional de Telecomunicaciones (UIT) y la empresa FIRST diseñaron una serie de simulaciones interactivas, donde los equipos conformados por los participantes compitieron entre sí cumpliendo tareas y roles. Todo ello con la finalidad de poner en práctica los conocimientos adquiridos durante los días previos.

HACKEAN RED SOCIAL DEL ECU 911 - ECUADOR

El Comercio - La noche del miércoles 18 de septiembre de 2024, ciberdelincuentes hackearon una de las cuentas de redes sociales del ECU 911, según detalló la entidad. El comunicado oficial informó que los atacantes vulneraron la cuenta de X, perteneciente a la Coordinación Zonal 5-8. El ECU 911 condenó el ataque y aseguró que presentará una denuncia ante la Fiscalía General del Estado. Además, el Servicio Integrado de Seguridad (ECU 911) explicó que los ciberdelincuentes accedieron a la cuenta de X de la Coordinación Zonal 5-8.

EL MINISTERIO TIC REFUERZA LA SEGURIDAD DIGITAL EN LAS ENTIDADES PÚBLICAS CON LA ACTUALIZACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - COLOMBIA

MINTIC - Ante el creciente riesgo de incidentes de seguridad digital que enfrentan las entidades públicas, el Ministerio TIC ha intensificado su compromiso con la protección de los activos informáticos y la garantía de la continuidad en la prestación de servicios a los ciudadanos. El Ministerio TIC, consciente de la vulnerabilidad digital de las instituciones del Estado, ha desarrollado políticas y estrategias que buscan garantizar el uso seguro y eficiente de las tecnologías de la información y las comunicaciones (TIC).

COLOMBIA AND THE UNITED STATES CHAMBER OF COMMERCE SIGN AN AGREEMENT TO PROMOTE TECHNOLOGICAL DEVELOPMENT IN THE COUNTRY

BNAmericas - Within the framework of the UN Future Summit taking place in New York, the ICT Ministry and the United States Chamber of Commerce signed a Memorandum of Understanding (MoU) that marks a new chapter of collaboration between the parties at the technology level. The agreement seeks to promote the recognition of experiences and best practices, to address key challenges focused on different areas, such as the digital economy, connectivity, artificial intelligence regulation and digital education. An alliance that continues to contribute to the digital transformation of Colombia and supports efforts to make the country a Digital Power.

EMBAJADA EE.UU. PATROCINA TALLER ESTRATÉGICO SOBRE CIBERSEGURIDAD CON EXPERTOS INTERNACIONALES - PARAGUAY

US Embassy - Expertos internacionales del Centro de Estudios de Defensa Hemisférica William J. Perry de los Estados Unidos de América, llevaron a cabo el Taller Estratégico de Ciberseguridad en la Universidad Metropolitana de Asunción (UMA), el 24 y 25 de setiembre, 2024, con el fin de promover un diálogo entre distintos sectores de la sociedad paraguaya, para fortalecer, junto con los expertos internacionales, la defensa digital y enfrentar los desafíos cibernéticos actuales y del futuro. Este taller organizado con el apoyo de la UMA, fomentó un entorno colaborativo centrado en temas de ciberseguridad, generando debates entre representantes de ministerios, del sector de seguridad, del sector financiero, de la academia y de otras instituciones afines de Paraguay.

QUÉ ES EL PACTO DEL FUTURO: LAS 56 ACCIONES QUE PROPONE LA ONU Y LOS PUNTOS QUE RECHAZA EL GOBIERNO DE MILEI

Infobae - "Argentina será un Faro de Libertad". Con esa definición, en el gobierno de Javier Milei celebraron anoche haber sido el único país que decidió salirse del "Pacto del Futuro", un acuerdo aprobado en la Asamblea General de Naciones Unidas con apoyo de 193 países, que estableció compromisos para reformar las instituciones internacionales y aplicar 56 acciones y más de 100 propuestas de cambio para garantizar el crecimiento, la igualdad y garantizar sociales, políticos y económicos para las generaciones presentes y futuras. También incluyó un extenso capítulo denominado "Pacto Digital", que plantea la necesidad de regular las redes sociales, las empresas tecnológicas y la inteligencia artificial.

GLOBAL CYBERSECURITY INDEX - ITU

ITU - The Global Cybersecurity Index (GCI) is a trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. As cybersecurity has a broad field of application, cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Development, and (v) Cooperation – and then aggregated into an overall score.

IN WAR AND SOCIETY, LARGE LANGUAGE MODELS ARE WHAT WE MAKE OF THEM

War on the Rocks - Prophecy and alarmism about AI are both overblown. No technology is a panacea or poses a risk independent of the people and institutions surrounding its use. Adapting algorithms to support strategic analysis requires studying the people, culture, and bureaucracy as much as it does model performance. War on the Rocks has been at the center of emerging debates about the roles, missions, and even ethics and morality of the growing integration of AI into the military. Every day, articles emerge highlighting either the game-changing possibilities of generative AI models or the perils associated with them. This trend is particularly acute with respect to large language models that synthesize large volumes of data to generate prompt-based responses that every reader has probably already played with, if not used in a professional setting.

MITIGATING AI-GENERATED DISINFORMATION: A CYBER COLLABORATIVE FRAMEWORK FOR G7 GOVERNANCE

Global Solutions - In an increasingly multipolar and conflict-prone world, witnessing the rise of artificial intelligence(AI), this paper explores the disruptive potential of AI-generated disinformation, a growing threat to global peace and security. The advance of generative AI tools able to rapidly produce convincing “synthetic disinformation”, such as large language models (LLMs), has exponentially amplified the reach and impact of foreign information manipulation and interference (FIMI) wielded by both state actors and non-state actors alike. Against this challenge, the G7 countries have shown proactive leadership in recognising and addressing the threat posed by AI and disinformation, leveraging resources and expertise to develop innovative strategies. Still, the lack of uniformity in regulatory approaches and policies across G7 nations, as well as the compartmentalisation between cyber policies and counter-disinformation responses, has resulted in fragmented solutions that are now insufficient. This paper argues that tackling AI-generated disinformation with a cyber-security approach not only offers an effective framework for G7 action but also paves the way for broader AI and cyber regulation milestones, leveraging the G7’s role as normsetter in peace, security and global governance.

WIFI SUSPENDED AT BIG UK TRAIN STATIONS AFTER ‘CYBERSECURITY INCIDENT’

The Guardian - Wifi networks at a number of train stations across the UK have been suspended after a “cybersecurity incident”. Nineteen stations including London Euston, Manchester Piccadilly and Birmingham New Street had their wifi services suspended on Wednesday night after the incident. They were still down on Thursday. The Manchester Evening News reported that passengers accessing the wifi at Piccadilly station were directed to a webpage titled “We love you, Europe”, which contained Islamophobic messages and details of several terrorist attacks that have taken place in the UK and in Europe.