DIGI AMERICAS ALLIANCE MEMBERS

COSTA RICA ACUSA A HUAWEI DE OBSTACULIZAR EL DESARROLLO DE REDES 5G

Infobae - El Gobierno de Costa Rica acusó este miércoles a la empresa Huawei de obstaculizar el desarrollo de las redes de quinta generación (5G) en el estatal Instituto Costarricense de Electricidad (ICE), uno de los principales proveedores de internet y telefonía móvil en el país. "La empresa Huawei coaccionando o tratando de obligar al Estado a no tomar en cuenta el decreto (sobre ciberseguridad) para que ellos se aseguren su participación. Esto lo hacen con el apoyo de dos sindicatos del ICE", declaró este miércoles la titular del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), Paula Bogantes.

HACKEO A CONSEJERÍA JURÍDICA DE SHEINBAUM CONTÓ CON 'SOCIO' MEXICANO: ESPECIALISTA EN CIBERSEGURIDAD

Aristegui Noticias - RansomHub, el grupo cibercriminal que presuntamente hackeo a la Consejería Jurídica de la Presidencia de México, ataca con apoyo de socios locales que podrían ser empleados o exempleados de la propia Consejería, advirtió el director de la empresa de ciberseguridad Nekt Group, Manuel Rivera. En entrevista para Aristegui en Vivo para hablar del hackeo al sitio de la Consejería Jurídica del Ejecutivo Federal (CJEF), Rivera explicó que ese “socio local” pudo proporcionar las credenciales y contraseñas a los hackers de RansonmHub, o bien, esas mismas credenciales pudieron haber sido obtenidas por negligencia de un funcionario o exfuncionario.

ENCUENTRO DE CIBERSEGURIDAD JUNTO A LA EMBAJADA DE ESTADOS UNIDOS - ARGENTINA

Argentina.gob - El evento, que consta de tres jornadas, se realiza en el marco de las acciones que la Dirección Nacional de Ciberseguridad viene llevando adelante para intervenir en la formulación y ejecución de planes de capacitación. En ese marco, se llevará a cabo un Tabletop Excersice, un juego de roles que sirve para trabajar en escenarios de riesgo y discutir las acciones conjuntas a seguir ante una emergencia. “La ciberseguridad es un eje clave que nos compromete a fortalecer nuestras instancias de cooperación internacional, ya que las amenazas digitales no respetan fronteras y evolucionan de manera constante, exigiéndonos innovar y adaptarnos para enfrentarlas”, sostuvo Genua en sus palabras de bienvenida.

HASTA $14,600 DE MULTA POR INFRINGIR LEY DE DATOS PERSONALES - EL SALVADOR

El Salvador - La Ley de Protección de Datos Personales aprobada el pasado 12 de noviembre por la Asamblea Legislativa también contempla multas económicas que van desde los $3,650 hasta los $14,600 para quienes cometan infracciones a dicha normativa. La nueva normativa se aplicará a toda persona natural o jurídica, pública o privada, que lleve a cabo actividades de tratamiento de datos personales. De acuerdo a las definiciones, el tratamiento de datos se entiende como: “Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales”. Estas se relaciona con la obtención, uso, registro, organización, conservación, difusión, almacenamiento, posesión, acceso, manejo y divulgación de datos personales.

MITIC HABILITA ESPACIO EN LÍNEA PARA CONSULTA PÚBLICA SOBRE EL BORRADOR DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2024-2028 - PARAGUAY

MITIC - El Ministerio de Tecnologías de la Información y Comunicación (MITIC) habilita un espacio de consulta pública para la construcción de la Estrategia Nacional de Ciberseguridad 2024-2028. Desde hoy, ciudadanos y profesionales paraguayos del ámbito de las tecnologías de la información y comunicación (TIC) pueden participar enviando sus comentarios, opiniones y sugerencias a través del Portal Paraguay. El anuncio lo hizo el director general de Ciberseguridad y Protección de la Información del MITIC, Jorge Levera, en compañía de la directora del CERT-PY, Diana Valdez, durante el KavaconPY, evento de Ciberseguridad organizado por expertos locales y disertadores internacionales en el Sheraton Asunción Hotel.

LA SIE TRABAJA EN PLAN DE RESPUESTA EN REGLAMENTO DE CIBERSEGURIDAD - REP. DOMINICANA

Diario Libre - El superintendente de Electricidad, Andrés Astacio, enfatizó la necesidad de fortalecer la ciberseguridad en el sector energético, dada la creciente amenaza de ataques cibernéticos que afectan a empresas eléctricas en todo el mundo. Astacio abordó la necesidad de establecer protocolos de acción claros y mecanismos de respuesta inmediata para proteger la infraestructura física y virtual del sistema eléctrico. "Estamos enfrentando miles de millones de ataques cibernéticos dirigidos a nivel mundial, y República Dominicana no es la excepción", por lo que consideró que cada segmento del sector eléctrico debe contar con sus mecanismos de acción.

SENADOR PUGH EXPUSO SOBRE LEY MARCO DE CIBERSEGURIDAD EN EL SENADO MEXICANO

Senado.cl - El senador Kenneth Pugh expuso sobre la Ley Marco de Ciberseguridad a la Comisión permanente de Seguridad Pública del Senado mexicano, en una sesión coordinada con la Academia Mexicana de Ciberseguridad y Derecho Digital; y la Alianza México-Ciberseguro, en el marco del segundo Foro de una iniciativa que busca crear una estrategia nacional de ciberseguridad, con leyes y normativas acordes a ella. El proyecto “Hacia una Estrategia Nacional de Ciberseguridad en México: Y principios para la legislación y regulación en ciberseguridad”, ha sido desarrollado en conjunto entre instituciones públicas y privadas, de forma colaborativa, intercambiando conocimientos y experiencias con el fin de fortalecer las políticas públicas en México, de una forma similar a la iniciativa chilena “Foro Ciber”.

AVANZA ACUERDO ENTRE URUGUAY Y ESTADOS UNIDOS POR TECNOLOGÍAS CRÍTICAS

DPL - Sesionó por segunda vez el grupo de trabajo bilateral que surgió del Memorando de Entendimiento con foco en tecnologías críticas firmado por Uruguay y Estados Unidos en abril pasado. Entre los temas clave del acuerdo se encuentran telecomunicaciones, Inteligencia Artificial, datos, flujo transfronterizo y ciberseguridad; también energía limpia, hidrógeno verde, biotecnología y semiconductores. En el marco de la cooperación, desde Uruguay destacaron la colaboración en el marco de ciberseguridad 2.0, el trabajo en gobernanza e IA y la integración de Uruguay a iniciativas globales de seguridad de datos y tecnologías limpias. “Realmente este acuerdo de cooperación nos permite fortalecer nuestras capacidades tecnológicas y económicas en áreas que son fundamentales para nuestro futuro”, señaló Elisa Facio, ministra de Industria, Energía y Minería de Uruguay.

LA CIBERSEGURIDAD Y EL ESPACIO FUERON ESCENARIOS IMPORTANTES PARA COLOMBIA, EN CRUZEX 2024

FAC - La ciberseguridad y el espacio fueron escenarios importantes para Colombia, en CRUZEX 2024 Durante el desarrollo de las misiones aéreas en CRUZEX 2024, se llevan a cabo de forma simultánea retos en los escenarios de ciberseguridad y la protección a la infraestructura espacial. Como parte del ejercicio CRUZEX 2024 que se lleva a cabo en Natal, Brasil, se crearon dos espacios para poner a prueba las capacidades de los integrantes de la Fuerza Aeroespacial Colombiana, así como la de algunos de los países participantes, en las áreas de ciberseguridad y protección a la infraestructura espacial, a través de retos diarios diseñados como ataques simulados a cada uno de los países participantes de estas mesas de trabajo, que día tras días generaron estrategias para lograr el objetivo de protección a sus activos, en ambos espectros.

5 WAYS TO ACHIEVE EFFECTIVE CYBER RESILIENCE

WEF - As economies worldwide adopt more digital technologies, ensuring protections against malicious cyberattacks, failures and outages continues to be a critical concern. And the challenge is a dynamic one – emerging technologies and increasing connectivity create a complex and moving backdrop. Today, many organizations’ primary goals and purposes are supported by technology-enabled business processes with no analogue alternative. This means that cyber resilience – an organization’s ability to minimize the impact of significant cyber incidents on its primary goals and objectives – can go beyond the digital sphere and not only affect service delivery but also stakeholder confidence and market position.

WE ASKED 4 TECH STRATEGY LEADERS HOW THEY'RE PROMOTING ACCOUNTABILITY AND OVERSIGHT. HERE'S WHAT THEY SAID

WEF - Digital trust has become increasingly important in the intelligent age, where technologies impact our everyday lives. The World Economic Forum’s Digital Trust Framework was created to help decision makers build societal trust by aligning around three core goals: security and reliability; accountability and oversight; inclusive, ethical and responsible use. In the second part of this series we focus on accountability and oversight, which requires organizations to take responsibility for trustworthiness through well-defined and clearly assigned specific stakeholders, teams or functions, along with provisions for addressing failures. Furthermore, it ensures that rules, standards, processes and practices are followed and performed as required.

HOW EMOTIONAL INTELLIGENCE IS THE BEST DEFENCE AGAINST GENAI THREATS

WEF - Imagine receiving a distressed call from your grandson; his voice filled with fear as he describes a horrible car accident. That's what happened to Jane, a 75-year-old senior citizen of Regina, Canada. Pressed by urgency, she was at the bank in a few hours, collecting bail money for her grandson. Only later did she discover she was a victim of an AI-generated scam. By 2030, GenAI is expected to automate 70% of global business operations, leaving leaders excited and fascinated. But there is a darker side to GenAI – the weaponization of its deception of people.

GUIDE TO CONDUCTING A NATIONAL PROLIFERATION FINANCING RISK ASSESSMENT: 2024

RUSI - RUSI's 2019 'Guide to Conducting a National Proliferation Financing Risk Assessment', the first of its kind, provided guidance to policymakers on identifying and responding to proliferation financing (PF) threats. Jurisdictions around the world have relied on the guide to understand key obligations, identify and assess PF threats, and mitigate risk. In the years since, much has changed in the world of PF. For one, the Financial Action Task Force (FATF), the international body responsible for setting anti-money-laundering standards, now requires its members to conduct national PF risk assessments as part of its mutual evaluation process. New technologies and payment platforms are also reshaping PF.