DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 8, 2024

DIGI AMERICAS ALLIANCE MEMBERS

INAUGURAN LABORATORIO DE CIBERDEFENSA PARA LA PROTECCIÓN DE INFRAESTRUCTURA CRÍTICA EN CHILE

EMOL - Gracias a una colaboración entre el Centro de Innovación UC y el Ejército de Chile, se inauguró el Laboratorio de Ciberdefensa para la Protección de Infraestructura Crítica, con la participación de destacados gremios y corporaciones empresariales. En este espacio, destinado a fortalecer la defensa de las infraestructuras críticas, participan entidades como la Asociación de Bancos e Instituciones Financieras (ABIF), la Corporación de Ciberseguridad Minera (CCMIN), el Coordinador Eléctrico Nacional (CEN), Conecta Logística del Ministerio de Transporte, CSIRT de Gobierno, la Universidad Católica a través de Dictuc - CETIUC, el Programa de Derecho, Ciencia y Tecnología UC, Duoc UC, y aliados tecnológicos como Siemens, Scitum Claro, Lab X2X Claro, Amazon Web Services, Palo Alto Networks, DreamLab y Thales

CRIMES CIBERNÉTICOS CRESCEM NO BRASIL E CIBERSEGURANÇA É DESAFIO PARA PRÓXIMOS ANOS

Tono Mural - A presença cada vez mais intensa da internet e das redes sociais em nossas vidas diárias é inegável. Dados do Instituto Brasileiro de Geografia e Estatísticas (IBGE) revelam que 82% dos domicílios brasileiros têm acesso à internet. O Brasil é ainda o terceiro país do mundo com maior uso das redes sociais. Fábio Matos, sociólogo especialista em perícia forense, ressalta a dualidade da comunicação digital. Embora a internet ofereça acesso à informação e oportunidades, também pode prejudicar quando usada de forma inadequada. "A comunicação digital é benéfica quando proporciona acesso à informação e capacitação. No entanto, é prejudicial quando leva à perda de contato com pessoas do cotidiano," afirma.

CHILE Y BRASIL FIRMAN ACUERDO DE COOPERACIÓN EN MATERIA DE CIBERSEGURIDAD

TrendTIC - En una ceremonia liderada por el Subsecretario del Interior, Manuel Monsalve, y Marcos Antonio Amaro Dos Santos, Ministro de Estado Jefe del Gabinete de Seguridad Institucional de la Presidencia de Brasil, ambos países firmaron en el Palacio de La Moneda un memorando de entendimiento (MOU), acuerdo de cooperación en materia de ciberseguridad entre ambos países. Lo anterior, en el marco de la Visita Oficial del Presidente Luiz Inácio Lula da Silva a Chile iniciada este 5 de agosto. El acuerdo destaca la necesidad de mejorar la preparación en ciberseguridad y gestionar riesgos, reconociendo la importancia de la cooperación internacional. Además, busca promover la cooperación y el intercambio de información, basados en valores compartidos y derechos humanos.

DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 8, 2024

COSTA RICA: MICITT E INA LANZAN PROGRAMA DE BECAS DE CIBERSEGURIDAD PARA MUJERES

Revista Summa - El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) y el Instituto Nacional de Aprendizaje (INA) anuncian el lanzamiento del programa «Analista de Ciberseguridad para su Negocio: Women», una iniciativa que ofrece 25 becas dirigidas a mujeres de pequeñas y medianas empresas (PYMES) y pequeños y medianos productores agropecuarios (PYMPAS). El programa tiene como objetivo fortalecer la seguridad digital de estas unidades productivas y fomentar la resiliencia empresarial en el entorno cibernético actual. Este programa, creado por mujeres para mujeres, no solo aborda las necesidades de seguridad cibernética, sino que también promueve la diversidad y la inclusión en el sector tecnológico. Las becas cubrirán el 95% del costo total del programa gracias a los recursos del INA, a través de su Programa General de Becas SBD. Cada empresa seleccionada deberá aportar el 5% restante, equivalente a ₡56,100.00.

MÉXICO LIDERA EN CRECIMIENTO DE DEMANDA DE ESPECIALISTAS EN CIBERSEGURIDAD

El Economista - En un contexto en el que la demanda de talento en ciberseguridad se enfrió a nivel global en el último año, México ha mostrado una tendencia a la inversa con un crecimiento en la búsqueda de estos perfiles especializados, de acuerdo con un análisis de LinkedIn Economic Graph. La demanda de talento tuvo un crecimiento anual de 6.8% durante 2024 en México, cifra que superó los niveles observados en economías como España, India, Países Bajos, Australia y Alemania, según los datos de la red profesional. En el caso de nuestro país, el comportamiento de la oferta de empleo en ciberseguridad está en línea con los riesgos percibidos por la alta dirección. El Digital Trust Insights 2024 de PwC muestra una preocupación de los ejecutivos en torno a las amenazas cibernéticas.

EL PARTIDO NACIONAL PRESENTÓ UNA DENUNCIA ATAQUE A SU PÁGINA WEB: "NO VAMOS A DEJAR PASAR NADA" - URUGUAY

El Observador - La presidenta del Partido Nacional, Macarena Rubio, se presentó este martes en la Unidad de Cibercrimen del Ministerio del Interior para denunciar el incidente de vulnerabilidad sufrido en la página web de la fuerza política en el que un grupo de ciberdelincuentes amenazaron a la senadora Graciela Bianchi. Mediante un comunicado mencionan que el ataque comprometió la seguridad de la web y aunque aseguraron que se implementaron medidas, la "gravedad del incidente" hizo evidente la necesidad de una intervención por parte de la Unidad de Cibercrimen.

GUÍA DE CIBERSEGURIDAD EN EL SECTOR ENERGÉTICO: CÓMO PROTEGER LOS DATOS Y EVITAR ATAQUES - REP. DOMINICANA

Energia Estrategica - En la República Dominicana, como en muchas otras partes del mundo, las empresas de generación de electricidad enfrentan riesgos significativos relacionados con la ciberseguridad tanto en sus Tecnologías de la Información (TI) como en las Tecnologías Operativas (TO). “Estos riesgos no sólo amenazan la estabilidad operativa de las empresas, sino también la seguridad nacional debido a la importancia crítica de la infraestructura eléctrica”, advirtió Elsa Encarnación, Directora de Ciberseguridad y Ciberdefensa del Ministerio de Defensa de República Dominicana.

DIGI AMERICAS LATAM CISO

INSIGHTS

AUGUST 8, 2024

CÓMO RESPONDE EL CENTRO NACIONAL DE SEGURIDAD DIGITAL ANTE CIBERATAQUES EN EL PERÚ

Andina - Un ataque de ransomware (secuestro de datos) que afectó en julio los servicios digitales del Ingemmet hizo retroceder los avances de simplificación administrativa, regresando al registro únicamente presencial de los petitorios mineros, y que -luego de dos semanas- aún no ha sido restablecido a nivel virtual. Afortunadamente, se logró resguardar el 100% de la información geológica y minera del país. Este ha sido uno de los más 380 incidentes de seguridad digital que este año han sido detectados y advertidos por el Centro Nacional de Seguridad Digital de la Presidencia del Consejo de Ministros (PCM). Conoce cómo funciona este equipo de expertos que acompaña a las entidades públicas y privadas en ciberseguridad.

AI COMPLACENCY IS COMPROMISING WESTERN SECURITY

ASPI - Just as the West has been forced into confrontation with Russia and China, military conflicts have revealed major systemic weaknesses in the US and European militaries and their defence-industrial bases. These problems stem from fundamental technology trends. In Ukraine, expensive manned systems such as tanks, combat aircraft and warships have proven extremely vulnerable to inexpensive unmanned drones, cruise missiles, and guided missiles. Russia has already lost more than 8,000 armored vehicles, a third of its Black Sea fleet and many combat aircraft, leading it to move its expensive manned systems farther from combat zones.

HOW TO MAKE MILITARY AI GOVERNANCE MORE ROBUST

War on the rocks - AI-enabled warfare has reached its “Oppenheimer moment.” From the backroom to the battlefield, AI is now being integrated into the full spectrum of military operations, including in logistics, intelligence collection, wargaming, decision-making, target identification, and weapons systems, with increasing levels of autonomy. The Ukrainian military is flying AI-enabled drones; the Israel Defense Forces are relying on AI to accelerate and expand targeting in Gaza; and the Pentagon is using AI to identify targets for airstrikes. The military AI revolution has arrived, and the debate over how it will be governed is heating up.

REFLECTING ON CYBER POWER: A LABOUR FUTURE?

RUSI - In 2021, the Integrated Review of Security, Defence, Development and Foreign Policy presented the UK’s ‘responsible, democratic’ view on cyber power that set out a strategic narrative and organising concept for future cyber policy. Amid the reassessment of priorities by the new government under its Strategic Defence Review, the concept and practice of cyber power must also be evaluated for its effectiveness. The Labour administration inherits a well-developed suite of strategic levers of cyber power, including institutions in the National Cyber Security Centre (NCSC) and the National Cyber Force (NCF) in addition to deep expertise across government. This commentary takes stock of the UK position on cyber power as a strategic narrative and organising concept, the challenges of promoting responsible and democratic use, and what this might mean for the new government.