LITORALPRESS

Fecha: 26-05-2025
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: UC y Ejército dan a conocer avances de CiberLab y anuncian creación de PP centro nacional de ciberdefensa

Pág. : 29
Cm2: 295,1

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

UC y Ejército dan a conocer avances de CiberLab y anuncian creación de centro nacional de ciberdefensa

Autoridades de la UC y del Ejército se reunieron en el Centro de Innovación UC.

A un año de la creación del Laboratorio de Ciberdefensa, buscan escalar la iniciativa con nodos regionales y nuevos socios.

POR MARCO ZECCHETTO

En julio de 2024, la Universidad Católica (UC) y el Ejército de Chile crearon el Laboratorio de Ciberdefensa para la Protección de Infraestructuras Críticas (CiberLab). La iniciativa, alojada en el Centro de Innovación UC Anacleto Angelini, reúne a representantes de los sectores público, privado y académico, para avanzar en gobernanza, pilotajes y generación de capacidades para proteger la infraestructura crítica.

Este jueves, en un evento previo a su primer aniversario, el rector de la UC, Juan Carlos de la Llera, anunció la consolidación futura del CiberLab como un centro con alcance nacional. "El CiberLab es también una plataforma para construir algo aún mayor: un futuro centro nacional de ciberdefensa que reúna capacidades tecnológicas, talento humano, estándares compartidos y visión estratégica con impacto nacional e incluso regional", dijo.

La subdirectora de Industrias del Futuro del Centro de Innovación UC, Rocío Ortiz, señaló que, para avanzar en esa dirección, sumarán nuevos socios -a los actuales 17- y articularán un modelo de gobernanza escalable a través de nodos del laboratorio en regiones.

Avances y focos

Respecto de los avances, Ortiz dijo que durante el segundo semestre de 2024 realizaron cuatro pilotos de ciberdefensa avanzada.

Entre ellos, una plataforma de indicadores de compromisos para integrar y procesar alertas de distintas fuentes y detectar patrones de amenazas relevantes por industria y un modelo de lenguaje grande (basado en IA generativa como DeepSeek y Llama de Meta) personalizado para uso interno en organizaciones, que permita analizar grandes volúmenes de datos sin comprometer información en servidores públicos.

También desarrollaron un software de ofuscación de código (modificación del código de fuente para aumentar su complejidad) para estudiar y realizar pruebas con *malware*, y un dispositivo de inyección de código para ingresar a redes aisladas o remotas.

Ortiz también destacó el primer ejercicio nacional de gestión de crisis que reunió a 150 instituciones, la capacitación de 320 uniformados y la participación de 1.000 personas en simulaciones de gestión de crisis y ejercicios técnicos.

Este año, el foco estará en la aplicación directa de los pilotos en sectores como banca y energía y presentar resultados, y en realizar nuevos ejercicios de simulación, como el primero enfocado en el sector eléctrico junto con el Coordinador Eléctrico Nacional.

También impartirán diplomados en ciberdefensa avanzada e integrarán inteligencia artificial a la plataforma de análisis de indicadores de compromiso.