LITORALPRESS

Fecha: 31-07-2025
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: CiberLab anuncia inédita iniciativa para evitar el hackeo de vehículos y nuevos proyectos de I+D+i

Pág. : 16
Cm2: 622,2

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

# CiberLab anuncia inédita iniciativa **para evitar el hackeo de vehículos** y nuevos proyectos de I+D+i

Cristián Guedelhoefer (Comandante del Ejército), Rocío Ortiz (directora CiberLab), María Angélica Fellenberg (UC), Claudio Araya (subsecretario de Telecomunicaciones) y Ramón Molina (Centro de Innovación UC), durante la ceremonia del primer año de aniversario.

**El Laboratorio de Ciberdefensa del Centro de Innovación UC y el Ejército, presentó los planes para 2025-2026, los que contemplan un Laboratorio de CiberMovilidad, aumentar pilotos y ampliar su presencia a nivel nacional.**

POR MARCO ZECCHETTO

El Laboratorio de Ciberdefensa para la Protección de Infraestructuras Críticas (CiberLab) fundado en julio de 2024, anunció este miércoles los planes para 2025-2026, los que incluyen una inédita iniciativa para proteger de hackeos a vehículos civiles, policiales y militares, proyectos de investigación, desarrollo e innovación (I+D+i) y ampliar su presencia a nivel nacional.

El CiberLab es una iniciativa del Centro de Innovación de la Universidad Católica (UC) Anacleto Angelini y del Ejército de Chile, para articular acciones de los sectores público, privado y académico para fortalecer la ciberseguridad de infraestructuras críticas, con pilotajes, generación de capacidades y gobernanza.

En su primer año de operación, el Laboratorio -alojado en el Centro de Innovación UC- coordinó con sus 17 socios una serie de proyectos. Entre ellos, cuatro pilotos en ciberdefensa avanzada; el primer ejercicio nacional de gestión de crisis de ciberseguridad con 150 instituciones; dos ejercicios dirigidos a equipos técnicos de respuesta, el primero en vulnerabilidades TI (tecnologías de la información) y el segundo, en OT (tecnologías operativas) con testeos críticos de un aeropuerto con maquetas y simuladores; además de capacitaciones a uniformados.

La subdirectora de Industrias del Futuro del Centro de Innovación UC y directora del CiberLab, Rocío Ortiz, destacó la consolidación y la "tracción" del modelo de trabajo conjunto durante su primer año.

"Es fácil firmar un convenio de colaboración, pero lo difícil es articular un primer portafolio con pilotos y dar continuidad al trabajo en conjunto. Construimos escenarios, enfocándonos en casos de uso reales y en los procesos, no en las tecnologías. Ahora está pendiente el escalamiento regional no solo en espacios físicos, sino a nivel de las capacidades y de talento. Estamos armando este modelo", dijo.

Comentó que, de los cuatro pilotos de ciberdefensa avanzada, el desarrollo de un modelo de lenguaje grande basado en IA generativa lo incorporó el Ejército para revisión de documentos privados. El segundo, una plataforma de indicadores de compromiso marcó el hito para la creación, en conjunto con el Ejército, de la Unidad de Análisis de Inteligencia de Amenazas del CiberLab. Y los otros dos -un software de ofuscación (para modificar código fuente y aumentar su complejidad) y un dispositivo de inyección de código para redes aisladas- están en testeo y escalamiento tecnológico.

## Un laboratorio de cibermovilidad

Entre las novedades, Ortiz anunció el primer Laboratorio Virtual de CiberMovilidad, una iniciativa en alianza con los grupos europeos Cybentia y Eurocybcar, enfocada en la protección de vehículos civiles, policiales y militares y que sería "la primera del mundo", afirmó.

**El Laboratorio de CiberMovilidad sería el "primero en el mundo" y busca adelantarse a las exigencias regulatorias europeas.**

Ortiz explicó que este proyecto busca anticiparse a exigencias regulatorias que ya se aplican en Europa y que en Chile no se están abordando, como elevar los estándares en temas de seguridad de vehículos, para hacer las adecuaciones tecnológicas necesarias.

"Estamos adelantándonos, estableciendo un estándar mucho más alto para poder testear temas de seguridad en vehículos; entender cuáles son las vulnerabilidades, las causas y los vectores de ataques que están teniendo; y qué consecuencias hay para el desarrollo de tecnologías, protección y estándares que se tienen que empezar a desarrollar, y eso impacta directamente en la industria", dijo.

La iniciativa contempla ejercicios de simulación remota y proyectos de I+D+i -como testeos en sensorización y conectividad experimental-, además de programas formativos en línea con certificaciones en ciberseguridad para flotas, vehículos eléctricos y peritaje forense automotriz; y cursos a medida para las Fuerzas Armadas, policías, fabricantes de vehículos y sector minero. "Buscamos capacitar a unas 500 personas en el primer año", afirmó Ortiz.

## Proyectos

Para el segundo año, el CiberLab duplicará los recursos a $ 2 mil millones, aportados por el Centro de Innovación UC y los socios.

Tiene cinco proyectos en desarrollo. Entre ellos, su nueva Unidad de Análisis de Inteligencia de Amenazas, que combinará capacidades analíticas y experimentales para desarrollar modelos avanzados de análisis, detección de patrones, generación de alertas y visualización de amenazas en infraestructuras críticas y sectores estratégicos.

También con el Ejército, está realizando testeos de conectividad y telecomunicaciones junto al laboratorio experimental de tecnología 5.5G, para casos de uso en seguridad fronteriza.

En infraestructura crítica, está trabajando con el Coordinador Eléctrico Nacional para crear un "CSIRT eléctrico", es decir un equipo de respuesta a incidentes de seguridad informática que usará tecnologías cuánticas para traspasar información, como reportes de incidentes, de forma segura.

En el sector financiero están testeando modelos de análisis de imágenes en tiempo real para prevenir conductas de riesgo en cajeros automáticos, y el primer semestre de 2026 iniciarán proyectos con las industrias sanitaria, minera y logística.

El plan para consolidarse como un centro nacional de ciberdefensa, partirá con la creación de dos nodos regionales en el norte y sur durante 2026, lo que considera infraestructura compartida, talento regional y vinculación con empresas locales.