LITORALPRESS

Fecha: 31-07-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: Centro de Innovacion UC inaugura laboratorio de ciberdefensa para infraestructuras criticas

Pág. : 27
Cm2: 636,9
VPE: $ 5.643.744

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

Centro de Innovación UC inaugura laboratorio de ciberdefensa para infraestructuras críticas

Es un espacio de colaboración donde se van a pilotear capacidades de ciberseguridad para actores de los sectores público, privado y academia.

POR MARCO ZECCHETTO ROCCO

Este martes se inauguró el Laboratorio de Ciberdefensa para la Protección de Infraestructuras Críticas (CiberLab) en el Centro de Innovación de la Universidad Católica (UC) Anacleto Angelini, un espacio que busca convocar a actores de los sectores privado, público y académico, para experimentar, pilotear y generar capacidades para proteger la inafraestructura crítica del país.

Se trata de una iniciativa conjunta del Centro de Innovación UC y el Ejército de Chile, en la que participan la Asociación de Bancos (ABIF), la Corporación de Ciberseguridad Minera, el Coordinador Eléctrico Nacional, Conecta Logística del Ministerio de Transporte, el Equipo de Respuesta ante Emergencias Informáticas de Gobierno, la UC, y Duoc UC, con el apoyo tecnológico de Siemens, Scitum, Lab XtoX Claro, Amazon Web Services, Palo Alto Networks, DreamLab y Thales.

La subdirectora de Industrias del Futuro del Centro de Innovación UC, Rocío Ortiz, explicó que el CiberLab apunta a responder a las amenazas cibernéticas emergentes y perfeccionar la capacidad para proteger los sistemas de conectividad, como "telecomunicaciones, transmisión eléctrica, infraestructura logística (por ejemplo portuaria) y de salud", dijo.

Se enfocará en proyectos de experimentación y simulación; en desarrollar y actualizar casos de uso, como protección de infraestructuras de control industrial; además de diseñar y ejecutar programas de capacitación.

El laboratorio, de 100 metros cuadrados, operará a través de dos nodos de ciberdefensa, uno orientado al trabajo con el Ejército, y un espacio de uso compartido entre el Centro UC y el resto de los actores. "Los nodos van a convivir en el mismo espacio, y contarán con pantallas interactivas y diversas tecnologías para hacer formación y capacitación avanzada para los distintos equipos", dijo Ortiz.

Áreas de trabajo

La ejecutiva explicó que definieron cuatro líneas de trabajo renovables a 12 a 15 meses: formación y competencias, proyectos y pilotos, difusión y comunicaciones y espacio e infraestructura.

En formación y competencias se realizarán seminarios, charlas, cursos, ejercicios prácticos y simulaciones de incidentes, donde el desafío, explicó Ortiz, es responder a las necesidades de las empresas, detectar brechas y "desarrollar metodologías y modelos para hacer una capacitación aplicada y pensada para enfrentar situaciones en la vida real".

En proyectos y pilotos, se habilitará un espacio de pruebas y desarrollo de proyectos de Investigación, Desarrollo e Innovación (I+D+i), en áreas como inteligencia artificial y aprendizaje automático, comunicaciones seguras, criptografía y seguridad cuántica, medicina militar y telemedicina, tecnología *blockchain*, Internet de las Cosas y seguridad de redes.

Ortiz adelantó que hasta ahora se definieron ocho pilotos para realizar entre el segundo semestre de 2024 y el primer semestre de 2025, entre ellos, pruebas de simulación de ciberdefensa y *ransomware* (secuestro de datos); el desarrollo de dos plataformas, una de monitoreo de indicadores de amenazas y otra de interoperabilidad para compartir información de *malware*; además de espacios de prueba con generadores de números aleatorios cuánticos y pruebas de conectividad experimental con tecnología 5G.

En difusión se enfocará en eventos abiertos, *showroom* tecnológico, y publicaciones científicas, en tanto, en la línea de espacio e infraestructura, facilitará a los actores acceso a *hardware*, *software* de monitoreo e infraestructura digital en la nube.

Ortiz explicó que para trabajar en estas áreas, crearán tres comités en I+D+i, capital humano y políticas públicas.

8
PILOTOS
YA ESTÁN DEFINIDOS PARA 2024 Y 2025

Sectores

El teniente coronel, Juan Pablo del Castillo, comandante del batallón de Ciberdefensa del Ejército, dijo que se centrarán en traspasar el conocimiento de la institución relacionada a inteligencia de amenazas -en riesgo, prevención y acción- para contribuir al desarrollo de profesionales en ciberseguridad.

En este contexto, dijo que se enfocarán en generar vínculos con la industria de defensa y en determinar cuál va a ser el rol "que vamos a tener ante el resto de la infraestructura crítica nacional".

En tanto, el oficial de seguridad de la información de la ABIF, Juan Downey, comentó que buscarán desarrollar y articular las capacidades de respuesta frente a crisis y amenazas, que tengan impacto tanto en la industria financiera, como en la nación.

"Una de las dimensiones que queremos desarrollar en conjunto con el laboratorio es la simulación de ejercicios de ciberseguridad intersectoriales. Eso va a poder medir la capacidad de respuesta de cada uno de los sectores, pero su piedra angular debe ser el compartir información y desarrollar inteligencia colectiva", comentó.