CENTRO DE INNOVACION UC
ANACLETO ANGELINI

DuocUC

Reporte de Impacto

2024-2025

CIBERLAB

Reporte de Impacto

2024-2025

"CiberLab es 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".

JUAN CARLOS DE LA LLERA M.
RECTOR
PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

"CiberLab aborda desafíos que contribuyen a la competitividad país, desarrollando soluciones que incorporan la seguridad desde su diseño".

La vinculación entre la academia, el sector público y el mundo privado ha sido, desde sus inicios, un pilar clave en la labor del Centro de Innovación UC Anacleto Angelini. En ese espíritu, celebramos con entusiasmo el primer año del laboratorio CiberLab, una iniciativa que encarna nuestra visión de crear espacios donde la innovación se ponga al servicio de desafíos estratégicos para el país.

CiberLab surge como un punto de encuentro para fortalecer la ciberdefensa nacional, poniendo a disposición infraestructura especializada, tecnologías emergentes y modelos de formación que desarrollan las competencias necesarias para enfrentar amenazas cibernéticas cada vez más complejas. Este primer año ha sido testimonio de cómo la colaboración puede traducirse en avances concretos para resguardar los sistemas y redes críticas que sostienen nuestra sociedad.

Desde el Centro, promovemos un ecosistema donde las soluciones innovadoras se construyen desde la excelencia, la colaboración y la responsabilidad. Abordamos desafíos que contribuyen a la competitividad país, que incorporan elementos de desarrollo territorial de futuro e integran elementos de tendencias emergentes y habilitantes, como la robótica, la IA avanzada y las Smart Cities, cuyas soluciones deben incorporar la seguridad desde su diseño. CiberLab es una manifestación de ese propósito, y un ejemplo de cómo la articulación efectiva entre distintos actores puede generar capacidades estratégicas de largo plazo.

Agradecemos profundamente a quienes han confiado en este proyecto y han sido parte activa de su desarrollo. Seguiremos trabajando con convicción para consolidar a CiberLab como un referente nacional e internacional en ciberseguridad, avanzando hacia una sociedad más segura, resiliente y preparada para los desafíos del futuro.

RAMÓN MOLINA C.
DIRECTOR EJECUTIVO
CENTRO DE INNOVACIÓN UC ANACLETO ANGELINI

"Nuestra labor no se limita al ámbito operacional, sino que se proyecta hacia el desarrollo de capacidades en los nuevos dominios, articulando esfuerzos con actores académicos y tecnológicos como CiberLab".

La instauración del CiberLab representa un hito transformador para nuestro país en el camino hacia la consolidación de capacidades nacionales frente al complejo y dinámico espectro de amenazas cibernéticas. Desde el Ejército de Chile hemos sido protagonistas de una experiencia pionera que vincula armónicamente la defensa, la academia, la industria y el Estado en torno a un propósito común: proteger nuestras infraestructuras críticas mediante el conocimiento, la colaboración y la innovación tecnológica.

Durante este primer año, hemos sido parte de avances concretos que fortalecen la resiliencia nacional a través de diversas actividades, las cuales permitieron validar modelos de toma de decisiones estratégicos, robustecer nuestras capacidades operacionales y fomentar el trabajo conjunto en escenarios de alta complejidad.

Específicamente, gracias al apoyo institucional, se desarrollaron ejercicios estratégicos y técnicos mediante simuladores físicos aplicados a infraestructura crítica, que permitieron poner en práctica conocimientos técnicos en entornos controlados, al tiempo que fuimos partícipes de capacitaciones que beneficiaron a más de 320 miembros de la Institución en áreas como ciberdefensa: auditoría, administración de redes y análisis.

El trabajo colaborativo del Ejército ha sido calificado como esencial para la planificación, ejecución y evaluación de cada uno de los escenarios proyectados, fortaleciendo las capacidades operativas y la preparación ante situaciones de alta exigencia. Por su parte, la participación de actores internacionales ha sido clave para acceder a tecnologías emergentes y tendencias globales que enriquecen nuestras capacidades nacionales, mientras que la interrelación de diversas instituciones académicas ha generado una masa crítica de expertos que proyectan la defensa hacia nuevos dominios.

Bajo la firme creencia que el Ejército constituye un componente estratégico para la competitividad nacional y la consolidación de capacidades en el ámbito de la Defensa, asumimos la responsabilidad de implementar y operacionalizar las soluciones derivadas de este esfuerzo interinstitucional, trabajando de forma integrada con otros actores responsables del resguardo de nuestra infraestructura crítica. Este desafío conlleva una mirada hacia el futuro, pues, como Institución, proyectamos continuar facilitando la generación de espacios colaborativos que nos permitan pilotear, testear y aproximarnos a tecnologías emergentes habilitantes.

En este contexto, el desarrollo y aplicación de tecnologías como la Inteligencia Artificial ya está transformando el entorno militar mediante sistemas de apoyo a la toma de decisiones, análisis predictivo de amenazas y automatización de procesos logísticos y operacionales. Estos avances, además de fortalecer las capacidades operativas, han generado un impulso significativo en el ámbito académico, lo que

redundará en beneficio de la formación profesional de las próximas generaciones de Oficiales y Suboficiales de nuestra institución a través del CiberLab.

Por otra parte, la computación y navegación cuántica están siendo exploradas por organismos internacionales para mejorar la precisión en sistemas de posicionamiento, comunicaciones seguras y sensores avanzados, y tecnologías de conectividad experimental, como redes LPI/LPD (Low Probability of Intercept/Detection) y sistemas de comunicación óptica espacial, las que avanzan hacia una etapa de maduración con potencial para revolucionar las operaciones multidominio, entendidas como aquellas que integran capacidades simultáneas y coordinadas en los dominios terrestre, aéreo, marítimo, espacial, cibernético y del espectro electromagnético.

Esta convergencia tecnológica busca fortalecer la interoperabilidad táctica que permite una respuesta más ágil, sincronizada y resiliente frente a escenarios complejos y amenazas híbridas. Como institución, aspiramos a integrar estas líneas tecnológicas en entornos como el CiberLab a través de la promoción del escalamiento de capacidades y la incorporación de nuevos actores al ecosistema nacional de infraestructura crítica, ya que nuestro propósito es sostener este camino de progreso, explorar nuevas fronteras en el ámbito tecnológico y consolidar alianzas que fortalezcan la resiliencia nacional frente a los desafíos presentes y futuros del ciberespacio.

En el entendido que esta visión nos permitirá mantenernos a la vanguardia en defensa digital, para el Ejército de Chile esta iniciativa se presenta mucho más que un proyecto tecnológico, es una expresión tangible de nuestro compromiso permanente con la seguridad nacional, la soberanía tecnológica, la cooperación interinstitucional y la innovación estratégica al servicio del país.

GDD CRISTIAN GUEDELHOEFER E.
COMANDANTE DE EDUCACIÓN Y DOCTRINA
EJÉRCITO DE CHILE

"¡La ciberseguridad depende de todas y todos! Este primer año ha confirmado que la colaboración interdisciplinaria y multisectorial es clave para robustecer las capacidades de ciberdefensa de nuestro país".

A un año de la creación del CiberLab, como Escuela de Informática y Telecomunicaciones de Duoc UC celebramos con orgullo ser socios fundadores de esta iniciativa estratégica junto al Ejército de Chile y la Pontificia Universidad Católica de Chile.

Este primer año ha confirmado que la colaboración interdisciplinaria y multisectorial es clave para robustecer las capacidades de ciberdefensa de nuestro país. Desde la mirada técnico-profesional, Duoc UC ha aportado con formación aplicada, talento joven y proyectos concretos que han demostrado gran impacto en escenarios de simulación, pilotaje y desarrollo de soluciones tecnológicas reales.

Los ejercicios realizados, como las simulaciones en tiempo real de ciberataques a infraestructuras críticas, han sido espacios formativos valiosos, donde nuestros estudiantes y docentes han colaborado codo a codo con expertos del sector defensa, académico y privado. Esta experiencia no solo fortalece la empleabilidad de nuestros egresados, sino que también contribuye activamente al bienestar de la sociedad.

Agradecemos profundamente a quienes han hecho posible este primer año de logros. Seguiremos adelante con responsabilidad, visión de futuro y pasión por la innovación, para consolidar un ecosistema nacional de ciberseguridad resiliente, inclusivo y conectado con los desafíos del siglo XXI.

ALEJANDRA ACUÑA V.
DIRECTORA ESCUELA DE INFORMÁTICA Y TELECOMUNICACIONES DUOC UC

CIBERLAB

CiberLab: camino a mitad de futuro | Espacio e infraestructura compartida | El primer año de CiberLab | PROYECTOS, PILOTOS Y PRUEBAS DE CONCEPTO: Análisis de inteligencia de amenazas | Desarrollo y optimización de tácticas... | Desarrollo de un sistema de análisis multimodal | Desarrollo de un simulador de ciberdefensa | Soluciones de conectividad móvil para zonas remotas

Socios fundadores de CiberLab

ROCÍO ORTIZ

SUBDIRECTORA DE INDUSTRIAS DEL FUTURO Y DIRECTORA EJECUTIVA DE CIBERLAB

CENTRO DE INNOVACIÓN UC ANACLETO ANGELINI

COD CRISTIÁN GUEDELHOEFER

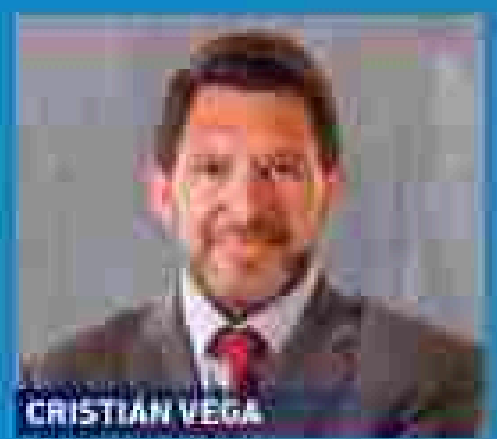
COMANDANTE DE EDUCACIÓN Y DOCTRINA

EJÉRCITO DE CHILE

SALVADOR VIAL

PRINCIPAL EJECUTIVE SECURITY ADVISOR

AWS



CRISTIAN VEGA

GERENTE DE OPERACIONES Y TECNOLOGÍA

ASOCIACIÓN DE BANCOS E INSTITUCIONES FINANCIERAS DE CHILE

MABEL LEVA

DIRECTORA EJECUTIVA

CONECTA LOGÍSTICA

PATRICIO LEYTON

DIRECTOR DE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA

COORDINADOR ELÉCTRICO NACIONAL

FELIPE BAHAMONDES

GERENTE GENERAL

DICTUC

RODRIGO RÍOS

DIRECTOR STRATEGIC ALLIANCE LATAM

DREAMLAB TECHNOLOGIES LATAM

FORMACIÓN Y DESARROLLO DE COMPETENCIAS

Escenarios de crisis: infraestructura crítica y toma de decisiones | Ejercicio de ciberdefensa Cuarto 2024 | Ejercicio de ciberdefensa Cuarto 2025 | Ejercicio CSIRT RTT 2025 | Cumbre de ciberseguridad | Seminario de ciberguerra | Diplomado y cursos | Talleres de ciberseguridad | Difusión y comunicaciones

ALEJANDRA ACUÑA

DIRECTORA ESCUELA DE INFORMÁTICA Y TELECOMUNICACIONES

DUOC UC

CLAUDIO ALCOTA

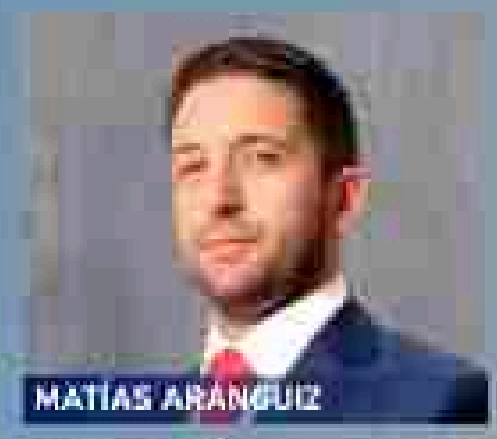
SUBDIRECTOR DE PROYECTOS ESCUELA DE INFORMÁTICA Y TELECOMUNICACIONES

DUOC UC

MAURICIO RAMÍREZ

COUNTRY MANAGER CHILE

PALO ALTO NETWORKS



MATÍAS ARANGUIZ

SUPERVISOR DEL PROGRAMA DIRECCIÓN DE SEGURIDAD

UNIVERSIDAD CATÓLICA

FRANCISCO GUZMÁN

PRESIDENTE ACTI

VICEPRESIDENTE DE

CLARO EMPRESAS

ALFREDO ROLANDO

SIEMENS INDUSTRIES

CYBERSECURITY REGIONAL MANAGER

SIEMENS

Partners de CiberLab

CENTRO DE INNOVACIÓN UC ANACLETO ANGELINI

AGUAS andinas

aws

banca

CCMIN

conecta logística

COORDINADOR ELÉCTRICO NACIONAL

CSIRT

dictuc CETIUC

DREAMLAB TECHNOLOGIES
Nicht glauben. Wissen.

Duoc UC

paloalto NETWORKS

Programa Derecho, Ciencia y Tecnología UC

Scitum

SIEMENS

THALES
Building a future we can all trust

Índice

CiberLab: contexto y visión de futuro

El laboratorio de ciberdefensa para la protección de infraestructuras críticas (CiberLab), es una iniciativa del Centro de Innovación UC y el Ejército de Chile, en conjunto con representantes de los sectores público, privado y la academia, cuyo objetivo es desarrollar un espacio asociativo neutral que permita abordar los desafíos de ciberseguridad y ciberdefensa de las infraestructuras críticas del país.

A partir de la promulgación de la Ley Marco de Ciberseguridad, han surgido como desafíos urgentes: la formación de competencias de carácter práctico, flexible, constante, actualizada y personalizada; el desarrollo de sandboxes y espacios de pilotaje; y el desarrollo de modelos de asociatividad con otros actores del ecosistema, que permitan compartir experiencias y aprendizajes actualizados.

En este contexto se inaugura CiberLab en julio de 2024, con la misión de robustecer el nivel de madurez y resiliencia de los sectores críticos nacionales públicos y privados, por medio de modelos asociativos de formación, pilotaje, difusión e infraestructura compartida. En el siguiente diagrama se muestran las cuatro líneas de acción que se trabajan colaborativamente entre los partners de CiberLab.

ESTRUCTURA Y LÍNEAS DE ACCIÓN

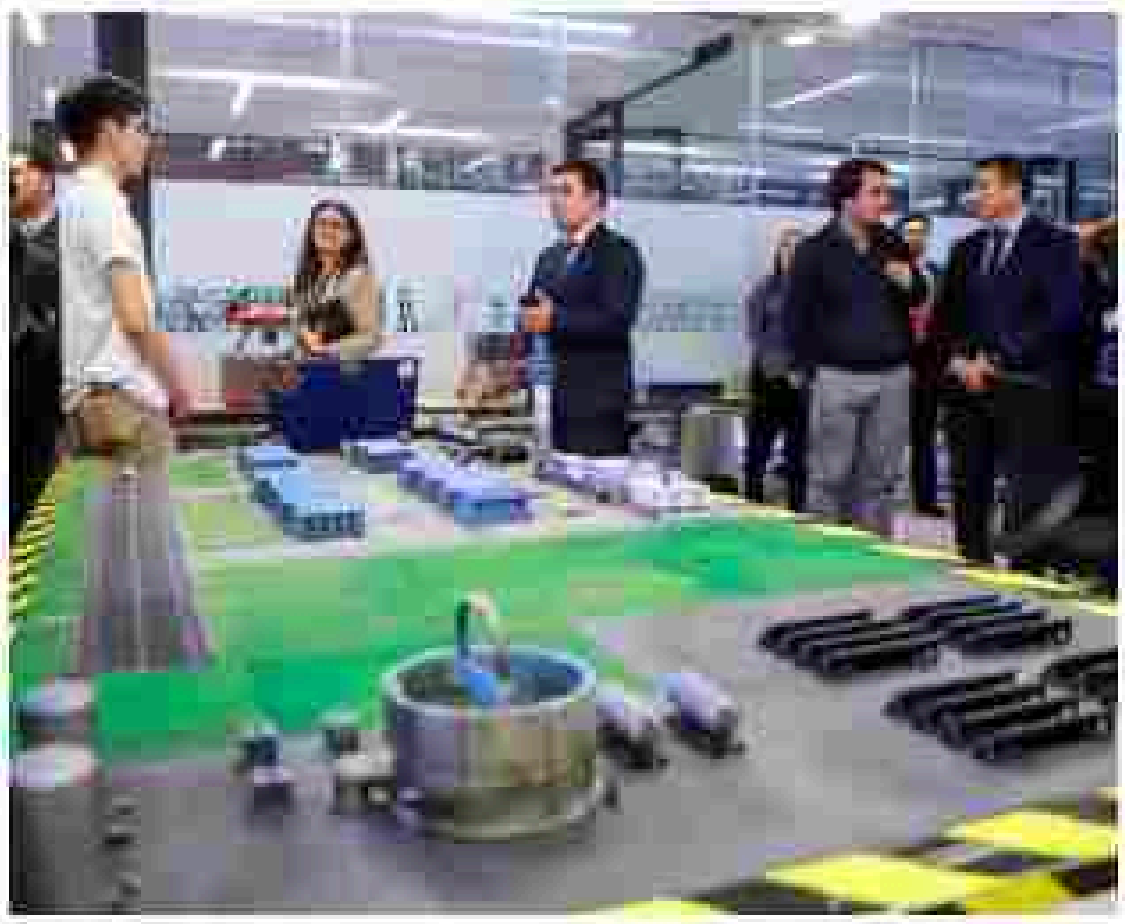
"Durante este primer año hemos logrado consolidar un ecosistema que convoca a los principales actores de los sectores de infraestructuras críticas del país en torno a la construcción de una visión audaz de futuro compartida: un país maduro y resiliente, que enfrenta las amenazas y riesgos cibernéticos a través de modelos de colaboración ágiles.

A futuro, proyectamos el escalamiento de este nodo de trabajo hacia un modelo nacional descentralizado que permita extender este portafolio de formación, tecnología y conocimiento hacia las distintas industrias y regiones a lo largo del país, posicionando a CiberLab, no sólo como un espacio nacional sino como un HUB regional de talento y tecnología para la ciberdefensa

ROCIO ORTIZ
DIRECTORA EJECUTIVA DE CIBERLAB

"Aún queda mucho por avanzar. La planificación para el segundo año proyecta una inserción más robusta de capital humano avanzado, el desarrollo de proyectos I+D con impacto institucional y el fortalecimiento de entornos de simulación y experimentación tecnológica en beneficio de la seguridad nacional".

CRL ROBERTO CASTILLO
JEFE CITEC EJÉRCITO DE CHILE



Sesión Ministerial de CiberLab en la ceremonia de cierre de curso

Espacio e infraestructura compartida

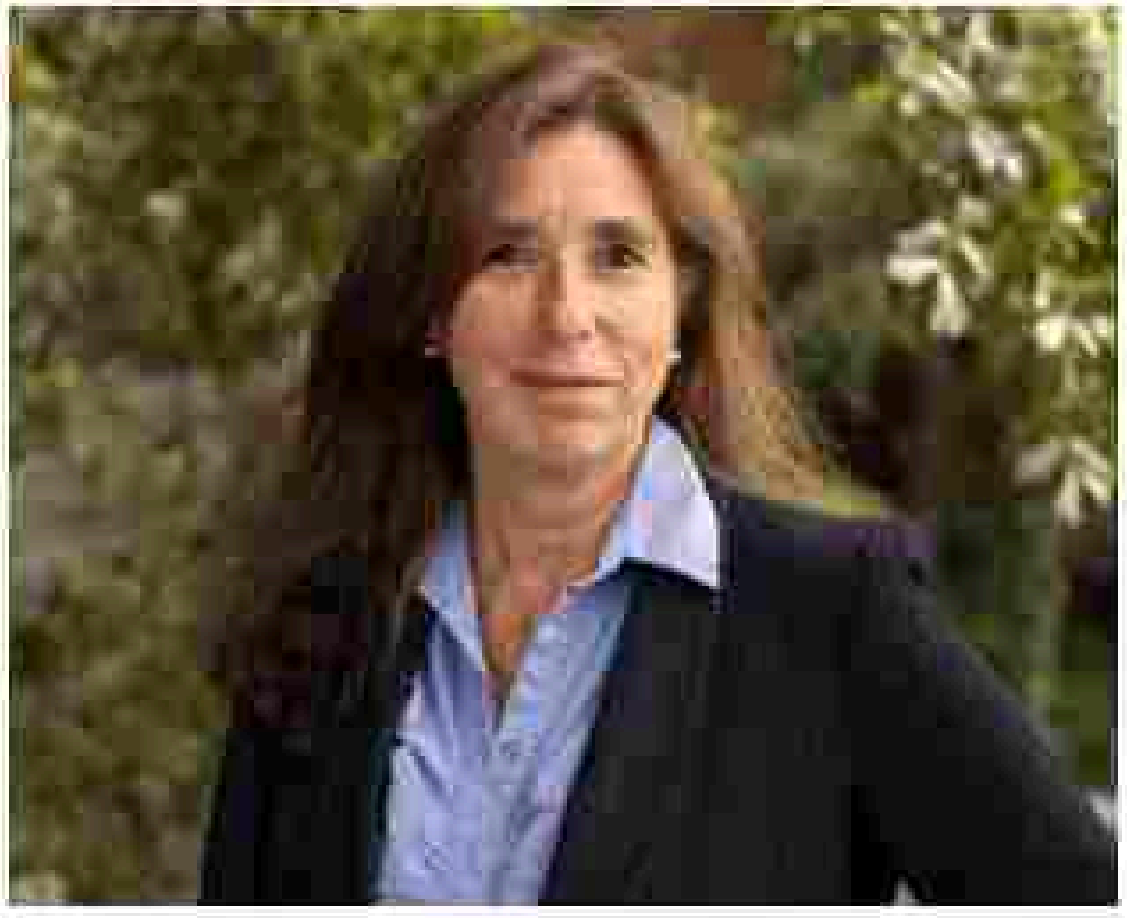
CiberLab proporciona instalaciones y recursos tecnológicos avanzados, como sandboxes y laboratorios, que permiten la investigación, entrenamiento y colaboración entre actores del sector público, privado y académico.


CIBERLAB

Corte de cinta en la ceremonia de inauguración de CiberLab. De izquierda a derecha en primer plano: Marcela Briones (Directora de Asuntos Corporativos y Comunicaciones del Centro de Innovación UC), Rodrigo Illia (Director Estratégico Alianzas LATAM de Dreamlab Technologies LATAM), Muriel Lara (Directora Ejecutiva de Cometa Logística), Cristián Quezada (Encargado de Educación y Doctrina del Estado de Chile), Pedro Bouchon (ex Vicerrector de Investigación UC), Cristián Vega (Gerente de Operaciones y Tecnología de ABIF), Alexandra Acuña (Directora Escuela de Informática y Telecomunicaciones del Duoc UC) y Ramón Molina (Director Ejecutivo del Centro de Innovación UC).

"Convertirnos en un orquestador a nivel nacional de tecnologías y pilotajes que terminan mejorando nuestra seguridad como país, es uno de los llamados de nuestra universidad y en especial de nuestro rector, quien reconoce las grandes capacidades de profundización e impacto que tiene el trabajo que ha desarrollado el equipo de este laboratorio".

MARÍA ANGÉLICA FELLENBERG
VICERRECTORA DE INVESTIGACIÓN Y POSTGRADO UC



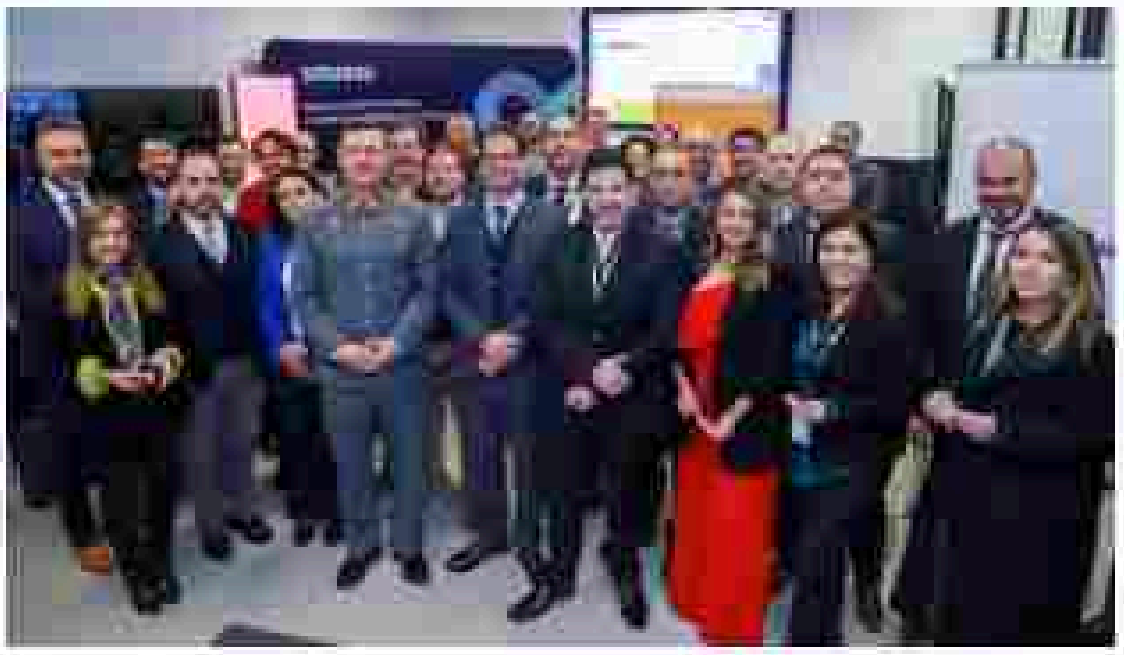
Inauguración

El 30 de julio de 2024 se inauguró el Laboratorio de Ciberdefensa para la Protección de Infraestructuras Críticas, CiberLab, con el fin de **proporcionar infraestructura compartida, recursos y un modelo asociativo de colaboración para facilitar el desarrollo de modelos de investigación aplicada, entrenamiento y transferencia de conocimiento entre actores del sector público, privado y académico, en torno a los desafíos de ciberseguridad y ciberdefensas del país.**

El laboratorio se compone de un espacio colaborativo que cuenta con *hardware* y *software*, sobre el cual se desarrollan pruebas de conceptos y pilotajes tecnológicos. Dentro de los equipos se cuenta con estaciones de trabajo de alto rendimiento para desarrollar procesamiento y análisis avanzado. Adicionalmente, se encuentra habilitado con infraestructura especializada como sensores, controladores y sistemas de automatización industrial, que son utilizados para el desarrollo de testeos en maquetas y simuladores con foco integración IT/OT.

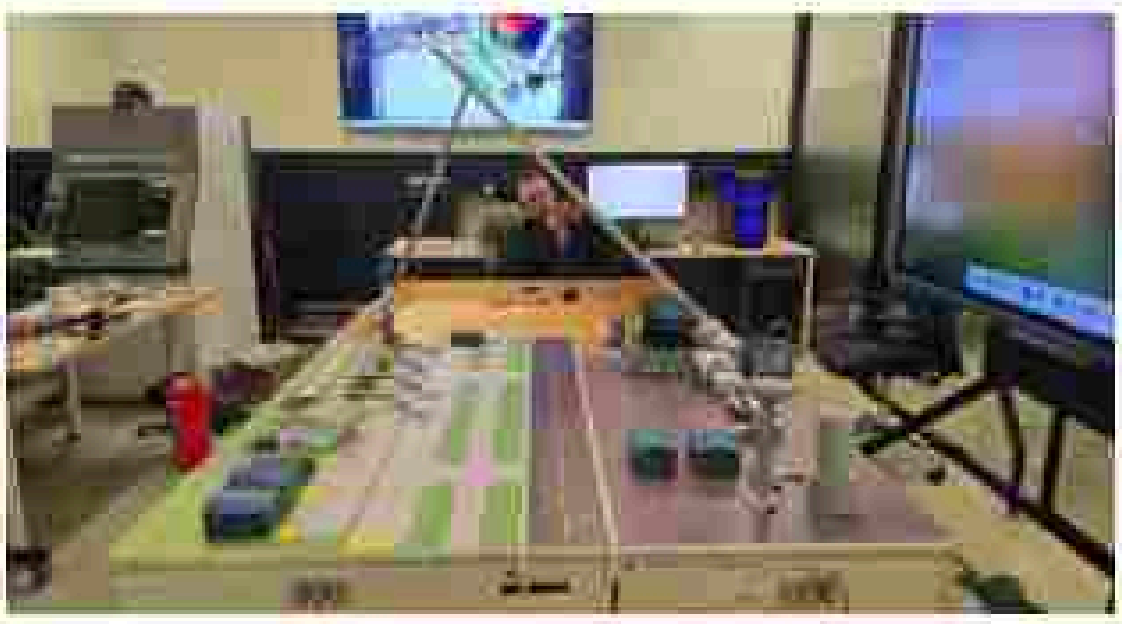
Los softwares utilizados en el laboratorio se enfocan en capacidades de análisis de inteligencia de amenazas y procesamiento de indicadores de compromisos. Así mismo, las capacidades del laboratorio permiten explorar las distintas capas del framework de ciberseguridad, pasando desde la identificación de amenazas, hasta la protección, detección, respuesta y recuperación luego de un incidente.

Junto con estos hardwares y softwares especializados, se han integrado herramientas complementarias para los análisis y desafíos de seguridad. Entre ellas destacan las tecnologías habilitantes y emergentes como la IA, ML, el análisis avanzado de datos, tecnologías cuánticas, los vehículos aéreos no tripulados (drones), la conectividad experimental 5G y 5.5G, entre otros.



Sesión Ministerial de CiberLab en la ceremonia de corte de cinta.

Panel "Desafíos público-privados de la ciberdefensa y la protección de infraestructuras críticas" realizado en el marco de la ceremonia de inauguración de CiberLab. El panel fue integrado por representantes de la Corporación de Ciberseguridad Minera, del Coordinador Eléctrico Nacional, de la Asociación de Bancos e Instituciones Financieras de Chile, y del Centro de Innovación UC.

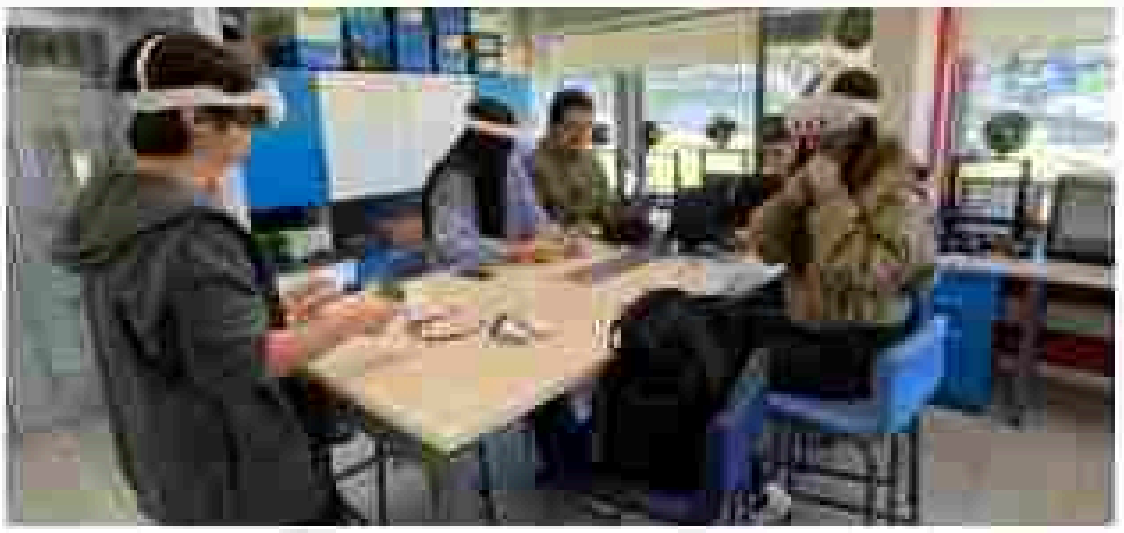


Despliegue de maquetas y simuladores OT.

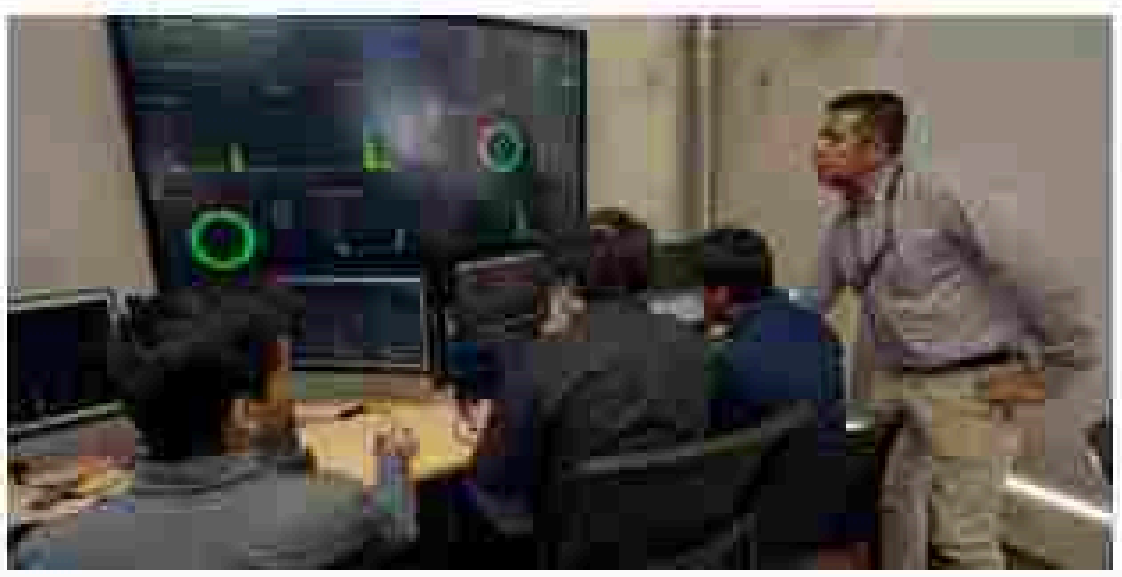
Dos nodos de ciberdefensa

CiberLab opera en torno a un modelo de trabajo de innovación dual, en el que **se integran los desafíos del sector civil, privado y público, con los desafíos de defensa frente a las amenazas cibernéticas**. De esta manera el laboratorio está diseñado en una modalidad colaborativa sobre 100 m2, donde se encuentran dos nodos de ciberdefensa, uno dedicado al trabajo del Ejército de Chile con el Centro de Innovación UC, y otro, al uso compartido entre los miembros fundadores del laboratorio y el Centro. Este modelo de articulación facilita el desarrollo de portafolios de trabajo especializados y la colaboración entre ambos nodos de trabajo.

Los nodos de ciberdefensa de CiberLab se vinculan con el HUB de tecnologías emergentes del Centro de Innovación UC, incluyendo el Laboratorio de Conectividad Experimental 5.5G, el Consorcio Conecta Móvil Lab, FabLab y Laboratorio de Industrias Creativas del Centro de Innovación UC, los cuales permiten ampliar las capacidades disponibles para explorar casos de uso interdisciplinarios y multiplataforma. Así mismo, los nodos UC se conectan con la red de laboratorios Duoc UC a nivel nacional, permitiendo una articulación de capacidades y talento transversal.



Centro de Innovación y Transferencia Tecnológica Duoc UC en Concepción.



Centro de Innovación y Transferencia Tecnológica Duoc UC en Viña del Mar.

Una de los equipos Duoc UC participando en el ejercicio Ciberlab 2024.

Red de laboratorios y talento Duoc UC

El **Centro de Innovación y Transferencia Tecnológica (CITT) – Duoc UC** es un espacio colaborativo que promueve la innovación, investigación aplicada y vinculación con el entorno productivo, fortaleciendo la formación práctica de los estudiantes. Está presente en 16 sedes y 2 campus, en las regiones de Valparaíso, Metropolitana, Biobío y Los Lagos, con equipamiento tecnológico avanzado, aportando A CiberLab una red de laboratorios.

Por otro lado, **CiberVoluntarios es una red de voluntarios que promueve una cultura en ciberseguridad y un uso responsable de dispositivos digitales**. Reúne a estudiantes, docentes, titulados y aliados del mundo público y privado para educar y acompañar a niños, jóvenes, personas mayores y comunidades vulnerables, fortaleciendo su confianza y seguridad en el entorno digital.

Ejército de Chile y Universidad Católica refuerzan alianza estratégica con encuentro en el Centro de Innovación UC

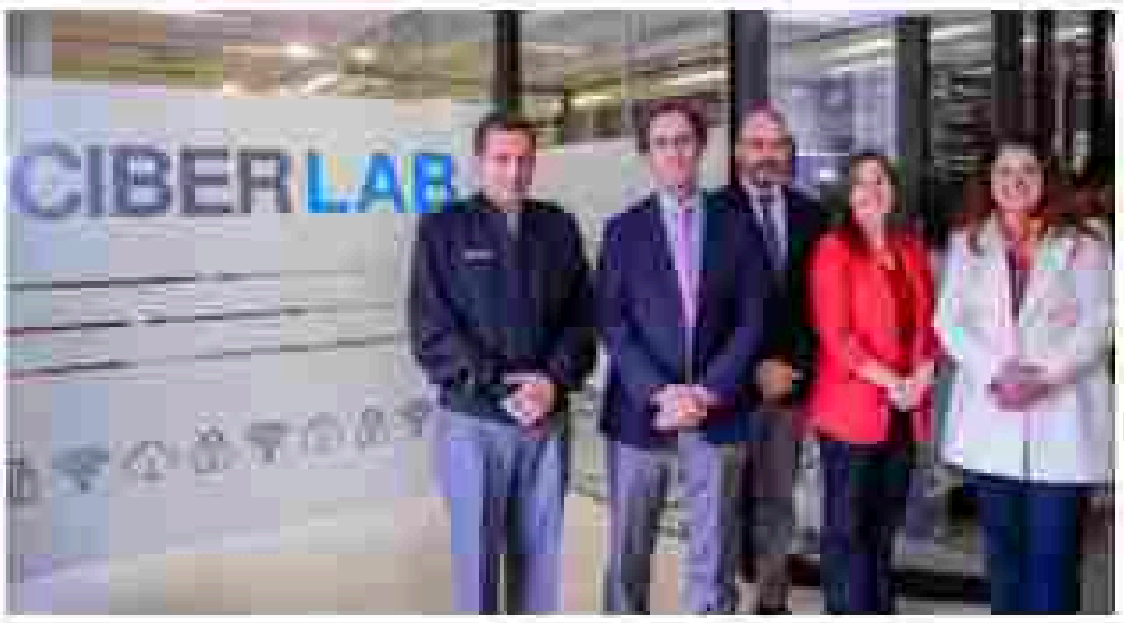
Como parte de uno de los nodos centrales de CiberLab, el Ejército de Chile junto a la UC han desarrollado por medio de su convenio de colaboración académica, un Laboratorio de Ciberdefensa especializado en los desafíos y oportunidades que la institución presenta en la materia. Este nodo cuenta con un portafolio de pilotos, proyectos y programas formativos diseñados a la medida para sus equipos de trabajo. Este nodo colabora con los actores del ecosistema compartiendo su experiencia y conocimiento para abordar los puntos comunes en torno a las amenazas emergentes.

"Los logros y avances de esta alianza competen la seguridad nacional y una mejora en las capacidades que tenemos como país frente a las amenazas cada vez más dúctiles a las que nos vemos enfrentados. Es por este motivo que el CiberLab sigue siendo una pieza fundamental en el crecimiento y especialización que muchos de nuestros efectivos militares han recibido durante este tiempo".

GENERAL DE EJÉRCITO JAVIER ITURRIAGA DEL CAMPO
COMANDANTE EN JEFE DEL EJÉRCITO DE CHILE

"CiberLab es 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".

JUAN CARLOS DE LA LLERA
RECTOR UC



Comandante en Jefe del Ejército de Chile, General de Ejército Javier Iturriaga del Campo, y el Rector de la UC, Juan Carlos de la Llera, en su visita oficial a CiberLab realizada el 22 de mayo de 2025. Los acompañan Ramón Molina (Director Ejecutivo del Centro de Innovación UC), María Angélica Fellenberg (Directora de Investigación y Postgrado UC) y Sonia Valladares (Decana de Ingeniería UC).

El primer año de CiberLab

CiberLab busca fortalecer la ciberseguridad y ciberdefensa de las infraestructuras críticas del país, promoviendo un entorno colaborativo y neutral que permite a expertos y organizaciones trabajar juntos en la protección de sistemas esenciales.

En su primer año de operaciones ha convocado a:

+1.000 Participantes

+150 Instituciones en actividades y ejercicios técnicos y estratégicos

+320 Uniformados capacitados

+50 Académicos, investigadores y estudiantes vinculados al desarrollo de pilotos

VER VIDEO

2024

30 de julio

Inauguración de CiberLab

02 de octubre

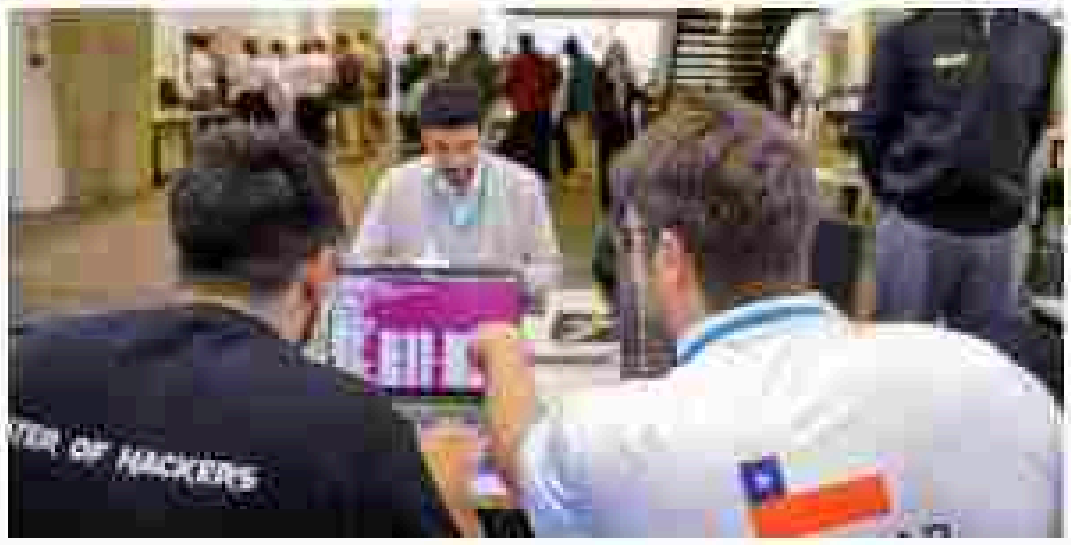
Seminario ciberguerra: escenario actual y tendencias

22 de octubre

Ejercicio estratégico: Escenarios de crisis, infraestructura crítica y toma de decisiones

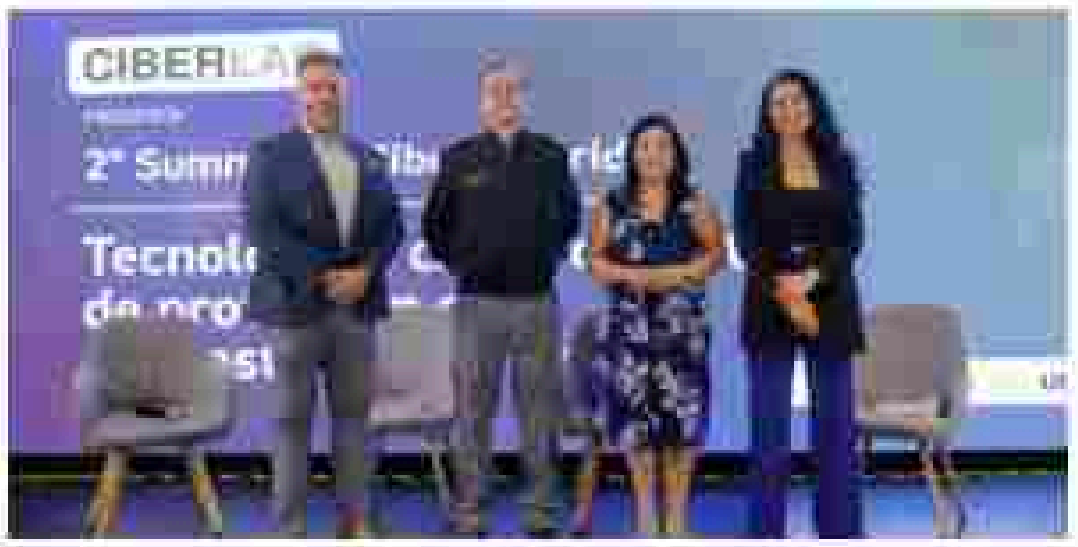
22 de octubre

Ejercicio de ciberdefensa Llaitún 2024: simulación de defensa IT/OT



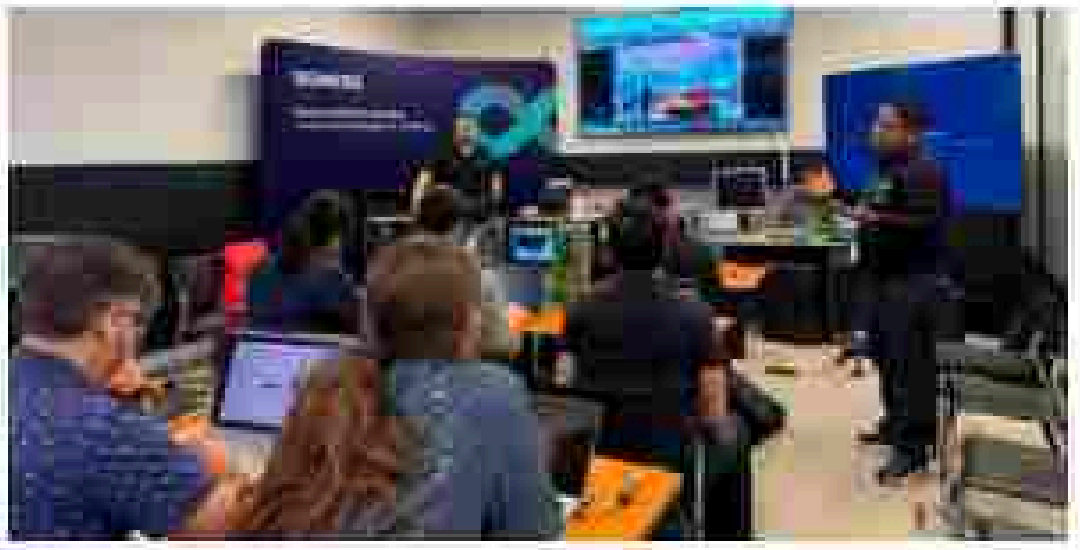
25 de noviembre

2° Summit de ciberseguridad: Tecnología y casos de éxito de protección de infraestructuras críticas



26 de noviembre

Taller de ciberseguridad OT



2025

22 de mayo

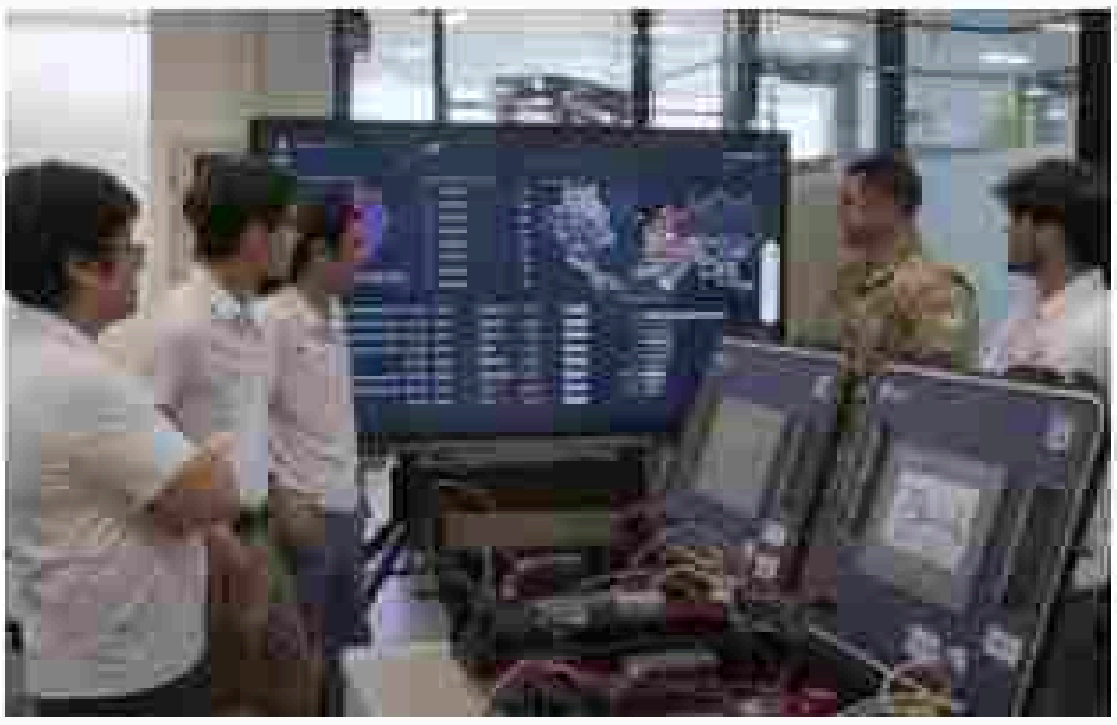
El Comandante en Jefe del Ejército de Chile y el Rector UC visitan CiberLab

23 de julio

CTF Llaitún 2025: OT warrior edition

Proyectos, pilotos y pruebas de concepto

Facilita el desarrollo de innovaciones tecnológicas y la implementación de soluciones piloto para ciberdefensa en infraestructuras críticas, fomentando un entorno de experimentación y validación.



Este primer piloto es la piedra angular para el desarrollo de la unidad de análisis de inteligencia de amenazas del CiberLab, con un fuerte enfoque en la integración de inteligencia artificial y análisis avanzado de datos aplicado a la ciberseguridad.

Análisis de inteligencia de amenazas

En el contexto de la línea investigativa de inteligencia de amenazas, durante 2024, el Ejército de Chile junto al equipo UC y sus partners, desarrolló análisis de indicadores de compromiso por medio de la integración de plataformas MISP y OPEN CTI. Esta iniciativa permite entender tendencias, actores y amenazas desde una perspectiva táctica y estratégica. Así, es posible trazar campañas, identificar patrones de ataque y alimentar procesos de gestión de riesgos y toma de decisiones.

Los objetivos de esta unidad son:

1. Desarrollar capacidades para la integración de fuentes de datos heterogéneas en un entorno centralizado.
2. Incorporar IA, aprendizaje automático y técnicas de correlación avanzada para la detección temprana de amenazas y patrones anómalos.
3. Fomentar líneas de investigación sobre amenazas emergentes e IA, en contexto de defensa cibernética.

Esta capacidad de análisis de datos permite en las próximas etapas del proyecto, la **detección de patrones de comportamiento malicioso** mediante modelos supervisados (se entrena a los modelos con IoCs ya clasificados para identificar nuevas amenazas similares) y no supervisados (se identifican clústeres de comportamiento anómalo).

Etapas del análisis avanzado usando IA y modelos de análisis de datos sofisticados que se proyectan como parte de las próximas líneas de investigación

Desarrollo y optimización de técnicas avanzadas en análisis de *malware*

Las unidades de análisis de ciberinteligencia enfrentan un desafío constante de identificar y mitigar amenazas provenientes de *malwares* y vectores maliciosos avanzados que podrían comprometer no sólo su infraestructura crítica, sino también la seguridad nacional.

A través de este piloto, el Ejército de Chile junto a equipo de estudiantes UC desarrollaron herramientas para mejorar la capacidad de análisis y respuesta. En particular, se analizó el impacto de la aplicación de inteligencia artificial en el análisis de *malwares*. Este tipo de iniciativas permite facilitar la comprensión de mecanismos avanzados utilizados por los cibercriminales en la actualidad y fortalecer las capacidades defensivas por medio del entrenamiento de la integración de tecnologías y modelos emergentes. Esto refuerza al personal especializado y contribuye al desarrollo de estrategias de defensa digital ante amenazas cada vez más complejas.

Además del impacto directo en el Ejército, el proyecto representa un avance relevante para la industria nacional de ciberseguridad, posicionándose como un esfuerzo pionero en el uso de IA para la defensa digital. Su valor radica en el potencial para prevenir ataques, proteger información crítica y fortalecer la soberanía digital del país.

"CiberLab fue clave como entorno de ensayo seguro para infraestructuras críticas, permitiéndonos simular escenarios reales de ciberataque. Esta experiencia, respaldada por la UC a través del programa SinLímites, fortaleció tanto mis habilidades técnicas como mi conciencia sobre los desafíos éticos en ciberseguridad.

Como desarrollador en el programa colaborativo, participé en el desafío enfocado en técnicas de identificación de malware, aplicando inteligencia artificial para automatizar análisis y explorar sus riesgos. Identificamos tendencias de generación de malware con IA que están realizando los cibercriminales con herramientas de libre acceso, las cuales representan amenazas crecientes".

PATRICIO ACEVEDO
ESTUDIANTE DE INGENIERÍA CIVIL INDUSTRIAL EN TECNOLOGÍAS DE LA INFORMACIÓN
UNIVERSIDAD CATÓLICA

Desarrollo de un sistema de análisis multimodal para documentación

Dentro de CiberLab también se incorporan el uso de tecnologías habilitantes y emergentes, como la IA y los modelos generativos. Durante el primer año se han realizado testeos de integración y análisis de su impacto en las operaciones actuales.

En el marco del trabajo diario de organizaciones como el Ejército de Chile y otras unidades de defensa y seguridad, el manejo de un alto volumen de datos e información sensible es de vital relevancia para el cumplimiento su misión. Esta información puede encontrarse en distintos tipos de archivos, estructurados y no estructurados, de texto, audio o imágenes.

En la actualidad existen diversos servicios de IA con chatbot incorporado que analizan documentos en línea como ChatGPT (OpenAI, 2025). De la misma manera, existen diversos servicios que permiten almacenar y administrar documentos, así como implementar inteligencia artificial usando recursos en la nube como AWS (AWS, 2025) y otros similares.

Sin embargo, dada la alta sensibilidad de la información, esta debe manejarse en un entorno local con extrema seguridad. Con el objetivo de facilitar el análisis de la información en distintos formatos, con los estándares de seguridad y confidencialidad necesarios, es que se levanta este desafío.

"Participar del programa SinLimites me permitió ampliar significativameote mis conocimientos, no solo en términos técnicos, sino también en habilidades interpersonales y de resolución de problemas. Este proyecto me dio la oportunidad de trabajar en un entorno multidisciplinario, colaborando con profesionales y estudiantes de distintas áreas, lo que enriqueció mi manera de abordar los desafíos. Además, me entregó una perspectiva distinta sobre cómo enfrentar los problemas: aprendí a considerar múltiples enfoques, a adaptar soluciones según el contexto y a valorar la importancia de la comunicación efectiva dentro de un equipo. Esta experiencia fortaleció mi capacidad de análisis, mi pensamiento crítico y mi iniciativa para proponer soluciones innovadoras ante problemas complejos".

FERNANDA ROMERO
ESTUDIANTE DE 9° SEMESTRE DE ASTRONOMÍA
UNIVERSIDAD CATÓLICA

Presentación del reto del desafío SimLumina, realizado en enero de 2025.

Desarrollo de un simulador de ciberdefensa para infraestructuras críticas en maquetas a escala

El piloto se enmarca dentro de las exigencias de la Ley Marco de Ciberseguridad en Chile, que establece la protección de infraestructuras críticas como una prioridad nacional. En un contexto donde la transformación digital ha incrementado la dependencia de tecnologías avanzadas, garantizar la confidencialidad, integridad y disponibilidad de la información es esencial para la operación segura de sistemas clave.

El objetivo del desafío consistió en diseñar e implementar un mecanismo de simulación de amenazas cibernéticas en la industria aeronáutica, con un enfoque en la prevención y gestión de riesgos asociados a accesos no autorizados internos y externos, a través del análisis de vulnerabilidades, simulaciones de ciberataques y desarrollo de estrategias de seguridad robustas y escalables.

El proyecto reviste una gran importancia para el Ejército de Chile, ya que busca fortalecer sus capacidades en ciberdefensa frente a un entorno de amenazas emergentes y complejas.

En particular, el simulador desarrollado permite modelar un caso de uso centrado en los sistemas de una cabina de vuelo, con el objetivo de evaluar y mitigar vulnerabilidades en sus sistemas. Su implementación representa un avance significativo en la preparación ante ciberataques y en la protección de infraestructuras críticas nacionales.

"El desarrollo del simulador representa un hito para nuestra institución y una apuesta concreta por la innovación aplicada a la protección de infraestructuras críticas. No solo permite simular ciberataques en un entorno controlado, sino que también fortalece la formación de nuestros estudiantes en áreas clave como ciberseguridad, sistemas SCADA y respuesta ante incidentes".

CRISTIAN BARRA
DIRECTOR DE CARRERA DE LA ESCUELA DE INFORMÁTICA Y TELECOMUNICACIONES DUOC UC

Soluciones de conectividad móvil para zonas remotas

Este desafío está en línea con lo que Chile enfrenta para brindar amplia cobertura de conectividad de última generación como el 5G/5.5G. Debido a su compleja geografía, condiciones territoriales y desastres climáticos, el alcance de cobertura puede verse limitado, especialmente en zonas extremas del país, lo cual limita la capacidad de respuesta de servicios esenciales. En este contexto, el objetivo principal del piloto fue investigar e identificar posibles soluciones para ampliar la cobertura 5G en zonas remotas, así como desarrollar herramientas que faciliten la toma de decisiones estratégicas orientadas a este fin.

"En este primer año, el CiberLab se ha consolidado como un espacio imprescindible para enfrentar los desafíos de ciberseguridad que exige el nuevo entorno digital. Su modelo colaborativo —que une Estado, academia e industria— ha permitido avanzar en pilotos concretos, formación especializada y construcción de capacidades estratégicas. Nos enorgullece ser parte de esta iniciativa que, desde su origen, impulsa una cultura de anticipación y resiliencia para proteger lo que es esencial: la infraestructura crítica del país".

FRANCISCO GUZMÁN
VICEPRESIDENTE
CLARO EMPRESAS

La relevancia del proyecto radica en el carácter crítico de la conectividad y cobertura a nivel nacional ante incidentes de ciberseguridad y su importancia transversal para el **restablecimiento del servicio frente a eventos disruptivos o emergencias.**

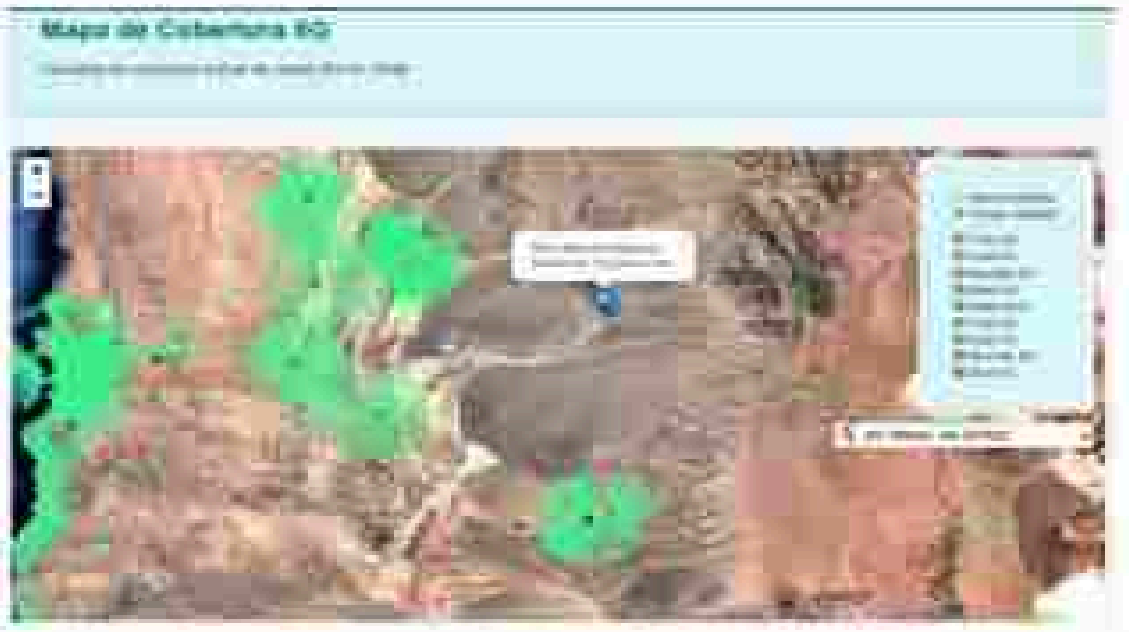
Como parte del proyecto, se trabajó en el desarrollo de diversas herramientas y en una **plataforma orientada a entregar información sobre el estado actual de la conectividad 5G, con un foco particular en la Región de Tarapacá.** Esta plataforma busca ser un insumo clave para identificar áreas críticas y evaluar **estrategias de expansión de la red** en el futuro.

De esta manera, CiberLab también explora la conectividad y las telecomunicaciones como habilitante de sus líneas investigativas en seguridad cibernética.

Presentación de cierre del desafío Sinlimites, realizada en enero de 2025.

"Trabajar con un equipo diverso de estudiantes de último año en modelar formas de conectividad en zonas rurales fue enriquecedor. Lo técnico se complementa con experiencias de cada uno para un resultado sorprendente".

ROLANDO MARTÍNEZ
DIRECTOR EJECUTIVO - XTEC



Formación y desarrollo de competencias

Orientado a capacitar profesionales en ciberseguridad mediante programas especializados, simulaciones y ejercicios prácticos, preparando a los equipos de respuesta ante incidentes en infraestructuras críticas.


EXIT:
Casos de éxito

Autoridades y participantes del evento realizado en Escuela Militar

Escenarios de crisis, infraestructura crítica y toma de decisiones

El Centro de Innovación UC, el Programa de Derecho, Ciencia y Tecnología de la UC, junto al Ejército de Chile, diseñaron y facilitaron el primer ejercicio estratégico de simulación de gestión de crisis cibernética para infraestructuras críticas, permitiéndole a los asistentes adquirir competencias para la gestión de crisis y levantamiento de buenas prácticas. Se utilizó el framework de trabajo NIST como base para diseñar una dinámica de roles en la cual los participantes tuvieron que enfrentarse a un proceso de toma de decisiones en un escenario de incidente crítico de ciberseguridad, aplicando las mejores prácticas conocidas en sus respectivas industrias.

Al inicio de la jornada los asistentes recibieron una inducción estratégica, a cargo de oficiales del Ejército de Chile, la cual les permitía familiarizarse con el escenario a desarrollar en el ejercicio. Esta fue seguida de una inducción técnica, liderada por el profesor Matías Aránguiz, dentro de la cual se profundizaba en la metodología y marcos de trabajo técnicos a utilizar durante la dinámica. Cada equipo de participantes contaba con el apoyo de un grupo de monitores ayudantes, estudiantes pertenecientes al Programa de Derecho, Ciencia y Tecnología UC.

En el ejercicio se analizó en profundidad el escenario de secuestro de datos y se evaluaron los modelos de gestión de crisis para la toma de decisiones de alto nivel, para la gerencias y áreas de empresas nacionales consideradas como infraestructura crítica.

+150

Representantes del sector privado, público, de la academia y del Ejército de Chile, quienes abordaron en equipos de gestión de crisis una situación de riesgo y vulneración de una institución de servicios esenciales financieros.

Multidisciplinario: cada asistente asumió un rol representando a distintas áreas estratégicas de la organización: legal, comunicaciones, tecnología y liderando la gerencia general. Debían resolver entre estudios y tareas asignadas durante la jornada, tomando decisiones de mitigación, haciendo reportería para las autoridades y dando declaraciones a la prensa, entre otras.

"Somos responsables de implementar y operacionalizar las soluciones técnicas y estratégicas que resultan de estas colaboraciones. El trabajo multidisciplinario con las infraestructuras críticas es fundamental para desarrollar una respuesta efectiva ante amenazas cibernéticas. Al integrar estas industrias en una red colaborativa de ciberseguridad, garantizamos que exista un flujo constante de información y mejores prácticas para detectar, mitigar y responder rápidamente a los ataques."

GENERAL DE DIVISIÓN RODRIGO MARCHESSI ACUÑA
COMANDANTE DE OPERACIONES ESPECIALES DEL EJÉRCITO DE CHILE

"La resiliencia digital se forja antes de que estalle la crisis. Cada incidente se transforma en conocimiento accionable: evaluamos el riesgo en tiempo real, anticipamos el siguiente movimiento y desplegamos respuestas sustentadas en datos. La gestión de crisis exige talento multidisciplinario capaz de contener, comunicar y restablecer operaciones, respaldado por marcos internacionales como NERC-CIP y MITRE ATT&CK. Solo mediante una estrategia de ejercicios de simulación, coordinación efectiva entre industria, academia y Estado podemos proteger los servicios esenciales y, en última instancia, salvaguardar a las personas".

PATRICIO LEYTON
DIRECTOR DE LA UNIDAD DE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA
COORDINADOR ELÉCTRICO NACIONAL

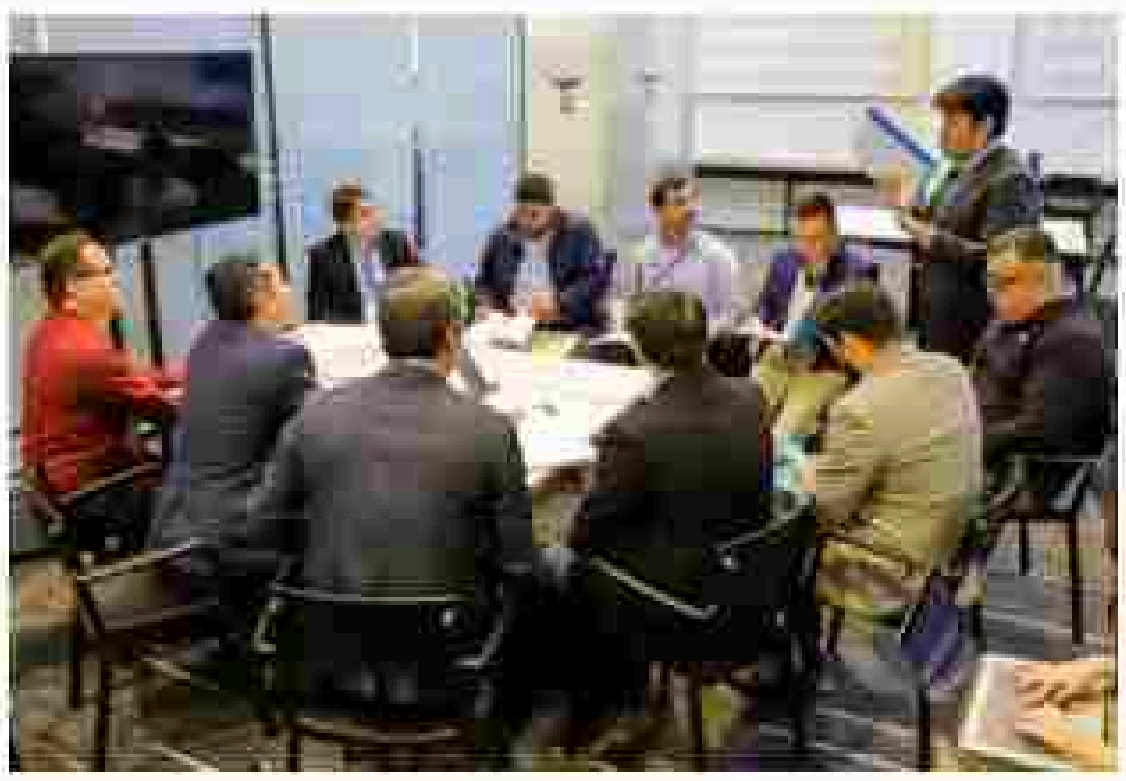
El trabajo en equipo les permitió a los asistentes conocer las mejores prácticas de análisis de la situación de incidente cibernético y abordar de manera multidisciplinaria una problemática que afectaría a toda la empresa, tal como sucede en un ataque real. Además, practicaron cómo exponerse ante los medios de comunicación internos y externos de la organización afectada.

Este hito se proyecta como el primero de una serie de jornadas de simulación y ejercicios prácticos que sirvan a la misión de robustecer las capacidades de resiliencia de los miembros del ecosistema de las infraestructuras críticas y operadores esenciales del país.

Claudia Cabrera, Líder en Customer Success Management Manager Chile & Perú de NCR Atleos participando en el ejercicio comunicacional.

"Dentro de una crisis no hay solo roles técnicos, quienes tienen marcos de respuesta estructurados, sino que también hay comunicacional, legal, de tomadores de decisiones, quienes cumplen un rol clave en la gestión de incidentes y son la cara frente a clientes, trabajadores, proveedores, etc."

MATIAS ARANGUIZ
PROFESOR DERECHO UC Y SUBDIRECTOR PROGRAMA DERECHO, CIENCIA Y TECNOLOGÍA UC



"Los diferentes sectores se verán potenciados gracias a la colaboración que, por medio del intercambio e integración de conocimiento, capacidades, experiencias y visiones, permitirán a cada organización que participe mejorar la capacidad de respuesta, pero lo más valioso se obtendrá de la generación de vínculos de confianza y de la integración de capacidades. La defensa en este ámbito debe ser colaborativa"

TCL JUAN PABLO DEL CASTILLO
ASESOR DE INTELIGENCIA DEL COMANDO DE OPERACIONES ESPECIALES DEL EJÉRCITO DE CHILE

Ejercicio de ciberdefensa Llaitún 2024: simulación de defensa IT/OT

Con el objetivo de integrar la dimensión técnica con la toma de decisiones, de forma paralela al ejercicio estratégico de gestión de crisis cibernética, se llevó a cabo el primer ejercicio táctico de ciberdefensa de infraestructuras críticas Llaitún 2024, en el cual se pusieron a prueba los conocimientos de los equipos técnicos de las instituciones, por medio de una serie de desafíos prácticos.

La actividad, realizada colaborativamente por el Centro de Innovación UC, DreamLab Technologies, Duoc UC y el Ejército de Chile, consistió en un ejercicio online dirigido a equipos técnicos de respuesta en ciberseguridad, basado en el modelo *Capture the flag* (CTF).

Este CTF combinó 14 desafíos, que debían ser resueltos de forma competitiva por los equipos, contra el tiempo, contando con alrededor de ocho horas para desarrollar el set de ejercicios completo. Los participantes abordaron diez ejercicios CTF tradicionales, junto a cuatro escenarios de infraestructura crítica simulada, con la tarea de defender una vulnerabilidad en un sistema o aplicación. Los desafíos CTF incluyeron actividades como análisis de *malware*, exfiltración de datos, escalada de privilegios, inyección SQL y *pentesting*, entre otros.

En el marco del 2° Summit de Ciberseguridad, realizado el pasado 25 de noviembre, cinco equipos (de Banco Estado, Banco de Chile, Duoc UC sede Viña del Mar y Banco Falabella) fueron premiados por su participación destacada en este ejercicio.

"El equipo técnico diseñó múltiples desafíos que abarcaron reversing, web, escalación de privilegios, entre otros, con distintos niveles de dificultad, ya que creemos firmemente que la ciberseguridad es una ciencia inclusiva: no importa cuanto sepas, siempre puedes aprender, crecer y enseñar. Nos enfocamos en crear un entorno innovador, sin miedo al fracaso, donde cada participante —principiante o avanzado— pudiera probar sus habilidades con confianza. Cada reto fue previamente testeado y el acompañamiento de nuestro equipo estuvo presente antes y durante toda la jornada para asegurar una experiencia fluida".

RODRIGO RIOS
DIRECTOR STRATEGIC ALLIANCES LATAM
DREAMLAB TECHNOLOGIES LATAM

"Simular ataques en entornos controlados con las herramientas para proteger la red nacional además de la configuración del despliegue y topología de red. La defensa comienza en el laboratorio".

BRUNO URREA
ESTUDIANTE DE INGENIERÍA EN CONECTIVIDAD Y REDES DUOC UC

+200

Participantes

+60

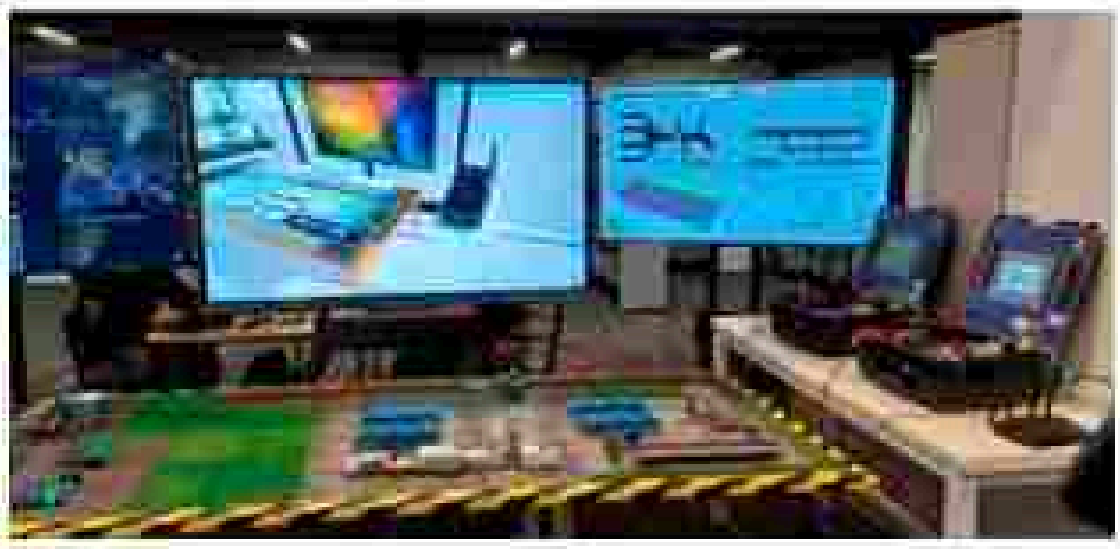
Equipos de todo Chile

14

Desafíos enfrentados

4

Escenarios de infraestructura crítica simulados



Ejercicio de ciberdefensa Llaitún 2025: *OT warrior edition*

El 23 de julio del presente año se llevó a cabo una edición especial del ejercicio táctico Capture The Flag (CTF), en el marco del primer aniversario de CiberLab. Esta versión, realizada colaborativamente por el Centro de Innovación UC, DreamLab Technologies, Duoc UC y el Ejército de Chile, se centró en la simulación de amenazas y respuesta ante incidentes en infraestructuras críticas con entornos de tecnologías operacionales (OT). Este tipo de tecnologías son fundamentales para las principales industrias productivas y servicios esenciales de nuestro país, de ahí la importancia de este ejercicio especializado. Ante un escenario en el cual se encontraba amenazada la integridad de una infraestructura nacional, representada por un aeropuerto y sus sistemas críticos, los equipos participantes debieron reaccionar rápidamente, tomando la iniciativa y actuando de manera ofensiva resolviendo amenazas comúnmente utilizadas por agentes maliciosos externos.

En la actividad se enfrentaron desafíos en torno a maquetas físicas representativas de sistemas críticos nacionales, desplegadas y operadas desde la Academia Politécnica Militar del Ejército de Chile, con la cual los participantes interactuaron remotamente a través de entornos controlados.

"Participar en el diseño de este CTF y ver a nuestros docentes y estudiantes competir junto a destacados actores del ecosistema, en un entorno avanzado de ciberdefensa, es una oportunidad única para vincular la formación técnica con desafíos reales en infraestructuras críticas. Esta experiencia potencia nuestras capacidades y reafirma nuestro compromiso con un entorno digital más seguro para el país".

ÓSCAR ARAYA T.
SUBDIRECTOR DE ÁREA ESCUELA DE INFORMÁTICA Y TELECOMUNICACIONES DUOC UC

"Este tipo de proyectos nos permite poner a prueba el cambio cultural que las empresas deben asumir con la nueva ley de ciberseguridad. Para nosotros como estudiantes, es una forma concreta de prepararnos para un futuro donde lo digital y lo operativo están cada vez más conectados".

MARCOS SEPÚLVEDA
ESTUDIANTE DE INGENIERÍA EN ELECTRICIDAD Y AUTOMATIZACIÓN INDUSTRIAL
DUOC UC

Ejercicio CTF VTF 2025

Equipos técnicos de CiberLab, junto a Dreamlab Technologies LATAM apoyaron el desarrollo y ejecución de un ejercicio táctico tipo Capture the Flag (CTF) para fortalecer competencias aplicadas y trabajo en equipo en contextos reales de ciberseguridad de la industria bancaria. En esta instancia participaron equipos de la Asociación de Bancos e Instituciones Financieras (ABIF) e invitados del Ejército de Chile, quienes trabajaron en un escenario colaborativo, desafiante y de alta exigencia.

A través de ejercicios como este, CiberLab impulsa el desarrollo de competencias estratégicas y técnicas para enfrentar los desafíos de la ciberseguridad, en un escenario colaborativo, desafiante y de alta exigencia.

Esta fue una instancia clave para fortalecer habilidades técnicas, pensamiento crítico y trabajo en equipo en contextos reales de ciberdefensa.

"Se implementaron 40 nuevos desafíos inspirados en problemáticas reales de la banca: errores típicos en acciones, compra-venta, cambios de divisas, interfaces de usuario, y más. Más allá del contenido técnico, lo más valioso fue el ambiente de trabajo que se generó. Gracias al liderazgo de CiberLab y al espíritu colaborativo de las y los involucrados, logramos construir un espacio seguro y motivador donde se fortalecieron vínculos y conocimos tanto las fortalezas como las debilidades de nuestro equipo."

RODRIGO RIOS
DIRECTOR STRATEGIC ALLIANCES LATAM
DREAMLAB TECHNOLOGIES LATAM

"Ser parte del ecosistema que está formando CiberLab es de alta importancia para la Asociación de Bancos e Instituciones Financieras. La participación en este tipo de ejercicios, no sólo permite acceder a una herramienta más para evaluar la capacidad técnica de la industria financiera, sino también compartir experiencia y priorizar objetivos. Además, participar en ejercicios con instituciones de otros sectores contribuye significativamente a generar lazos y fortalecer la resiliencia del ecosistema digital en su conjunto".

CRISTIAN VEGA
GERENTE DE OPERACIONES Y TECNOLOGÍA ASOCIACIÓN DE BANCOS E INSTITUCIONES FINANCIERAS DE CHILE

+200 Asistentes presenciales

+100 Seguidores online

60 Empresas / Organizaciones participantes

2° Summit de ciberseguridad: Tecnología y casos de éxito de protección de infraestructuras críticas

En el contexto del trabajo realizado en su primer cuatrimestre de operaciones, CiberLab desarrolló un robusto portafolio de trabajo y pruebas de concepto representando distintos casos de uso. Estos se dieron a conocer en el "2° Summit de ciberseguridad: Tecnología y casos de exito de protección de infraestructuras críticas", dando cuenta de la relevancia de la colaboración entre el sector público, privado y académico para abordar los desafíos en ciberseguridad.

El CISO de Aguas Andinas, Juan Huechucura, expuso como caso de exito los detalles de su experiencia en la protección de los servicios sanitarios, los cuales son parte esencial de las infraestructuras críticas.

En la actividad se realizó un panel de conversación para abordar desafíos que surgen en materia de ciberseguridad y los avances realizados por CiberLab. En el que participaron representantes de AWS, Buuc UC y el Ejército de Chile.

En la jornada, expusieron representantes del Coordinador Eléctrico Nacional y de Siemens. Además, se entregaron reconocimientos a cinco equipos multidisciplinarios que participaron en el ejercicio de ciberdefensa "CTF Llamin 2024".

"Compartir la experiencia y mejores prácticas con distintas industrias en este tipo de instancias, es sumamente relevante para robustecer las capacidades del ecosistema y la resiliencia de las infraestructuras críticas. Esto fomenta la generación de nuevos espacios asociativos y escenarios de nuevo conocimiento".

JORGE REBOLLEDO
LÍDER DE CIBERINTELIGENCIA DE LA INDUSTRIA
ASOCIACIÓN DE BANCOS E INSTITUCIONES FINANCIERAS DE CHILE

"Mi participación en el Summit 2024 reafirmó la importancia de iniciativas como Cibertab en el fortalecimiento de nuestras ciberdefensas. En un momento en que la Ley Marco de Ciberseguridad y la ANCI requieren capacidades técnicas y humanas sólidas, organizaciones como esta juegan un rol protagónico en un ecosistema donde debemos estar al día, competentes y conscientes de los desafíos actuales".

JUAN HUECHUCURA
CISO AGUAS ANDINAS

"Poder conocer de primera fuente las experiencias de otros países en situaciones similares permite que se puedan adaptar y mejorar nuestras propias capacidades, asimismo esto se une a la colaboración integral con otros actores nacionales relacionados con la administración de infraestructura crítica, permitiendo generar discusiones profundas para generar confianzas y realizar trabajos colaborativos de primer nivel que vayan en beneficio del resguardo de los intereses nacionales"

GENERAL DE DIVISIÓN CRISTIAN GUEDELHOEFER ERBETTA
COMANDANTE DE EDUCACIÓN Y DOCTRINA DEL EJÉRCITO DE CHILE

Seminario ciberguerra: escenario actual y tendencias

En el contexto del mes de la ciberseguridad, en la Academia de Guerra del Ejército de Chile se realizó una jornada de análisis, en la que **André Reichaw- Prehn, Socio Director EMEA (Centro y Sur) y LATAM de Palo Alto Networks Unit 42**, profundizó en los tipos de amenazas cibernéticas y organizaciones criminales que se ocultan en la web, realizando ataques transnacionales que pueden poner en riesgo las estabilidades políticas y sociales de otros países.

Tomando como referencia la guerra entre Rusia y Ucrania, André explicó cómo las estrategias de defensa digital deben apuntar a la protección de infraestructura crítica, considerando el sector de telecomunicaciones, eléctrico, logístico y financiero, entre otros. Esto demuestra **cómo los ataques cibernéticos realizados en el otro extremo del mundo podrían replicarse en nuestros sistemas nacionales**. Estas amenazas urgen a todos los actores públicos, privados y de defensa a compartir sus experiencias y perspectivas para configurar una protección de estos activos y fomentar la resiliencia nacional.

El expositor se sumó posteriormente al panel "Desafíos de la Ciberguerra e Infraestructuras Críticas", integrado por representantes del Ejército de Chile, del Coordinador Eléctrico Nacional, y del Programa Derecho, Ciencia y Tecnología UC.

Con este evento se posicionó una temática especializada como la ciberguerra en un entorno colaborativo, y se abordó el crecimiento exponencial de los riesgos a medida que se facilita la integración con tecnologías como la IA, que habilita nuevos diseños de ataques cibernéticos alrededor del mundo.

"Hoy, el mercado atraviesa una acelerada transformación digital, impulsada por tecnologías como la inteligencia artificial, la nube y la automatización, que están redefiniendo los modelos industriales. En este contexto, Palo Alto Networks ha destinado recursos en software, equipamiento e ingeniería para apoyar el desarrollo del Laboratorio, a través de pruebas, integraciones, capacitaciones y diversas actividades colaborativas".

MAURICIO RAMÍREZ BEYA
COUNTRY MANAGER PALO ALTO NETWORKS

Diplomado y cursos

Como parte del portafolio de trabajo del CiberLab, uno de los ejes centrales es el desarrollo de **programas de formación especializados**, que incluyen diplomados y cursos diseñados a la medida de las necesidades del ecosistema.

Estos programas se construyen en base a las **competencias prácticas requeridas por los equipos técnicos y estratégicos** que los cursarán, personalizando tanto los contenidos como las actividades formativas. Además, se selecciona cuidadosamente a los instructores, priorizando a **profesionales destacados con experiencia práctica actualizada** en los ámbitos de ciberseguridad y defensa digital.

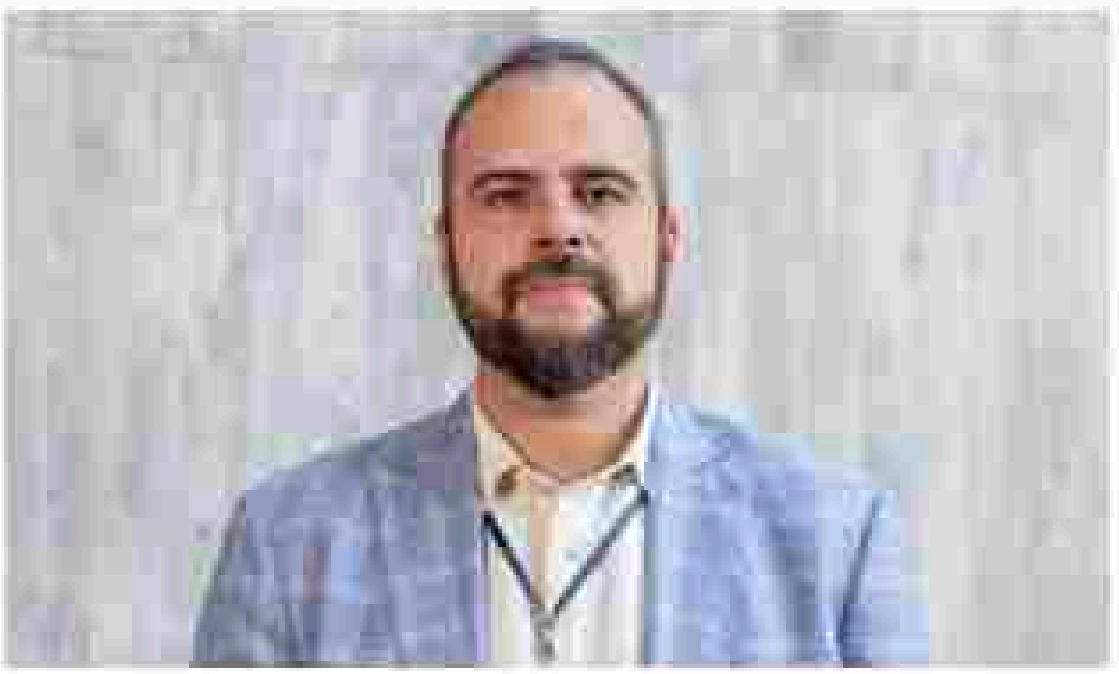
Actualmente, estos programas contemplan un perfil altamente orientado a la **aplicación práctica y técnica de alto nivel**, con estándares de exigencia acordes a escenarios reales. A la fecha, se ha logrado capacitar a **más de 320 uniformados** en diversas áreas, que van desde la auditoría de sistemas TI hasta habilidades de **ciberdefensa avanzada**.

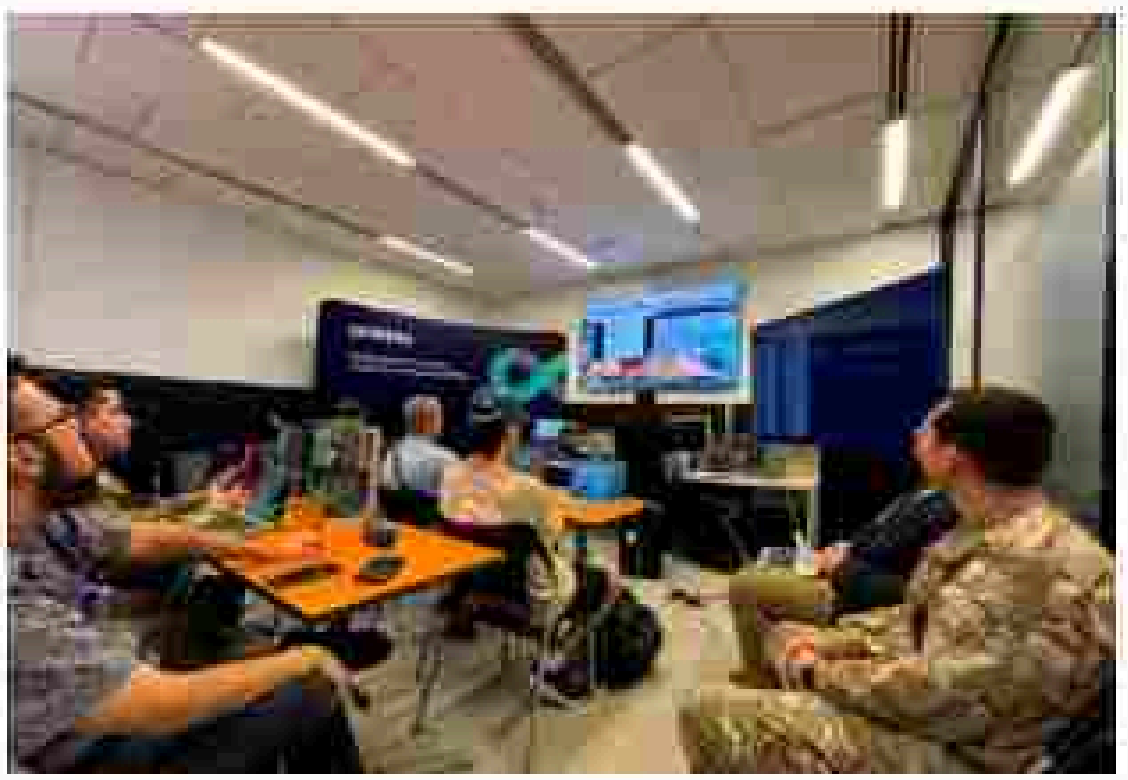
CRL ROBERTO CASTILLO
JEFE SITEC
EJÉRCITO DE CHILE

"Gracias al Convenio Marco suscrito en agosto de 2024 por el Ejército de Chile y la UC, ambas instituciones han confirmado una plataforma de cooperación académica orientada al desarrollo de capacidades estratégicas, articulando formación especializada, asesoría técnica, investigación aplicada y transferencia tecnológica. Así, durante este periodo, se han formalizado mecanismos específicos que han permitido ejecutar programas de formación en ciberdefensa, pasantías multidisciplinarias, talleres con enfoque innovador y el diseño de proyectos colaborativos que entrelazan saber militar y conocimiento científico".

"Desde CETIUC, aportamos conocimiento, experiencia docente y diseño instruccional para dar vida a los programas de formación de CiberLab. Esta colaboración permitió implementar cursos altamente especializados que hoy fortalecen las capacidades de ciberseguridad del país".

CARLOS ROJAS
DIRECTOR DE DESARROLLO ESTRATÉGICO Y ACADÉMICO
CETIUC





Talleres de ciberseguridad

Los Laboratorios de concientización en ciberseguridad industrial de Siemens son un caso de éxito en relación a los talleres impulsados por CiberLab y tienen como objetivo transformar la seguridad operacional.

Estos laboratorios representan una actividad estratégica crucial en el panorama actual de amenazas digitales. A través de la capacitación práctica, las organizaciones pueden proteger sus activos críticos, mantener operaciones continuas y construir confianza con sus stakeholders, mientras cumplen con las regulaciones vigentes.

En un mundo donde las amenazas cibernéticas evolucionan constantemente, estos laboratorios se convierten en una herramienta esencial para la preparación y respuesta ante incidentes, ofreciendo un retorno tangible en la reducción de riesgos y la mejora operacional.

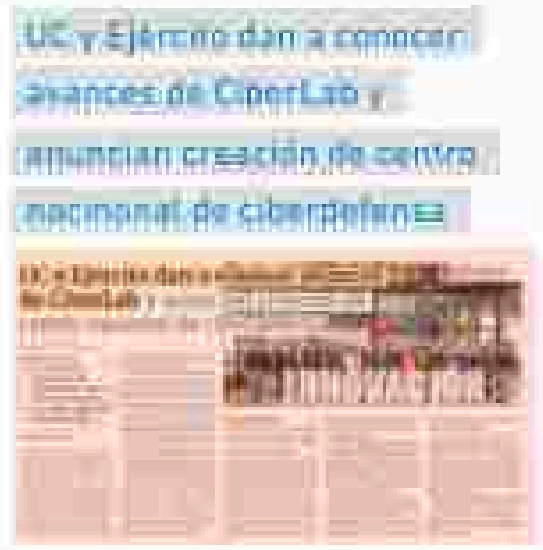
"Estos laboratorios de Siemens ofrecen un entorno controlado donde las organizaciones experimentan y aprenden a enfrentar amenazas cibernéticas reales. Esta experiencia práctica fortalece la resiliencia operacional, reduce riesgos y protege activos críticos, asegurando la continuidad del negocio y el cumplimiento regulatorio"

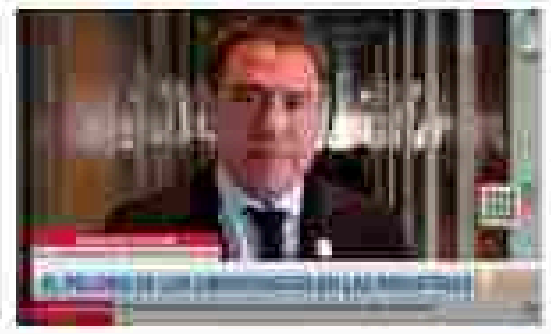
ALFREDO ROLANDO
DIGITAL INDUSTRIES CYBERSECURITY REGIONAL MANAGER
SIEMENS

Difusión y comunicaciones

Uno de los objetivos de CiberLab es promover el conocimiento en ciberseguridad a través de eventos académicos, publicaciones científicas y colaboraciones interinstitucionales, fortaleciendo la cultura de seguridad en el ecosistema. A continuación se presenta una selección de apariciones en medios de comunicación durante el primer año de operaciones del laboratorio.

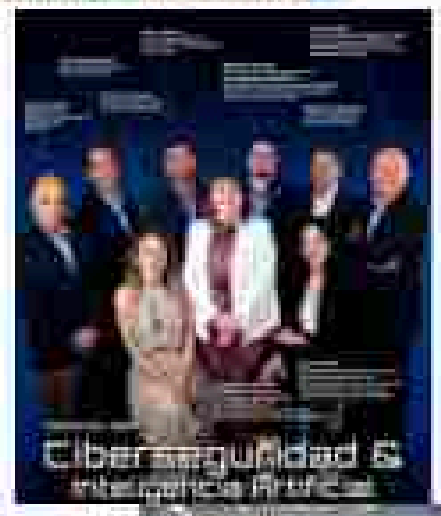

La gestión de crisis es un músculo que debe entrenarse


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

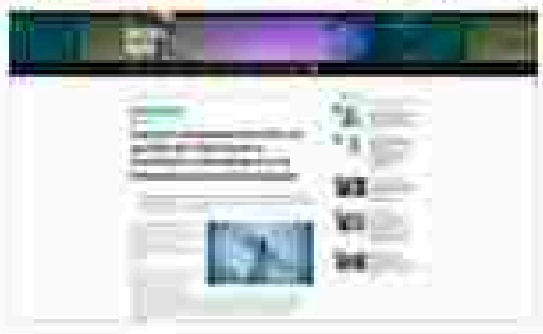

El peligro de los ciberataques en las industrias

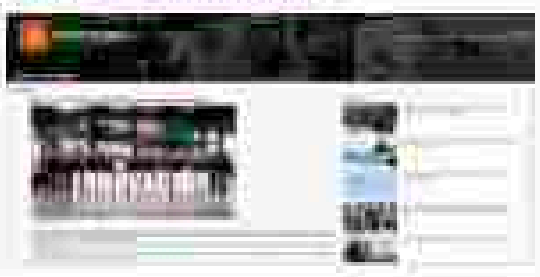

¿Cuáles serán los desafíos en ciberseguridad para Chile en 2025?


La colaboración público privada y de la academia es clave para fortalecer la resiliencia nacional frente a amenazas cibernéticas


Especial 2024 ciberseguridad e inteligencia artificial


Centro de Innovación UC inaugura laboratorio de ciberdefensa para infraestructuras críticas


Expertos analizaron desafíos en gestión de crisis frente a eventuales ciberataques a la infraestructura crítica del país


Ejército de Chile y Universidad Católica refuerzan alianza estratégica

Cybertech South America 2025

Falta de expertos en ciberseguridad urgen nuevos modelos educativos más STEM e inclusión de mujeres

Nuevas exigencias legales aumentan la demanda de talentos en ciberseguridad

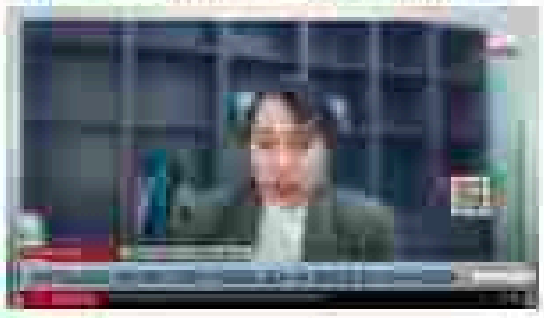
Analizan los desafíos de ciberseguridad para responder a eventuales crisis en la infraestructura crítica del país

Siemens es reconocida en los Premios AHK 2025 por su contribución a la innovación tecnológica y la ciberseguridad en Chile

Cómo fue el primer simulacro de ciberataque de infraestructuras críticas

Ciberdefensa: esencial para validar la infraestructura crítica

Las amenazas cibernéticas que acechan al sector minero



Las amenazas en el ciberespacio crecen de forma exponencial.
Nuestra mejor defensa:
hacer crecer los espacios de colaboración.

El viaje de CIBERLAB recién comienza

¡Súmate a la red de colaboración!

CIBERLAB

Reporte de Impacto

2024-2025

Santiago, julio 2025

Desarrollo de contenidos, redacción y edición
Rocío Ortiz, Subdirectora de Industrias del Futuro del Centro de Innovación UC y Directora Ejecutiva de CiberLab
Claudio Alcuta, Subdirector de Proyectos Escuela de Informática y Telecomunicaciones de Duoc UC
Coronel Raúl Rosas Álvarez, Director de Comunicaciones Estratégicas del Ejército de Chile
Pamela Silva, Coordinadora de Branding y Proyectos del Centro de Innovación UC
Florina Mescoso, Coordinadora de Proyectos y Gestión del Centro de Innovación UC

Fotografía
Photoadvisor.cl
Archivo fotográfico del Centro de Innovación UC
Se agradece a quienes facilitaron imágenes para este documento.

Diseño y diagramación
(F21.cl)
Agencia de Branding MarcaFuturo

Impresión
Imprenta MMG

CIBERLAB

ciberlab.uc.cl

ciberlab@uc.cl