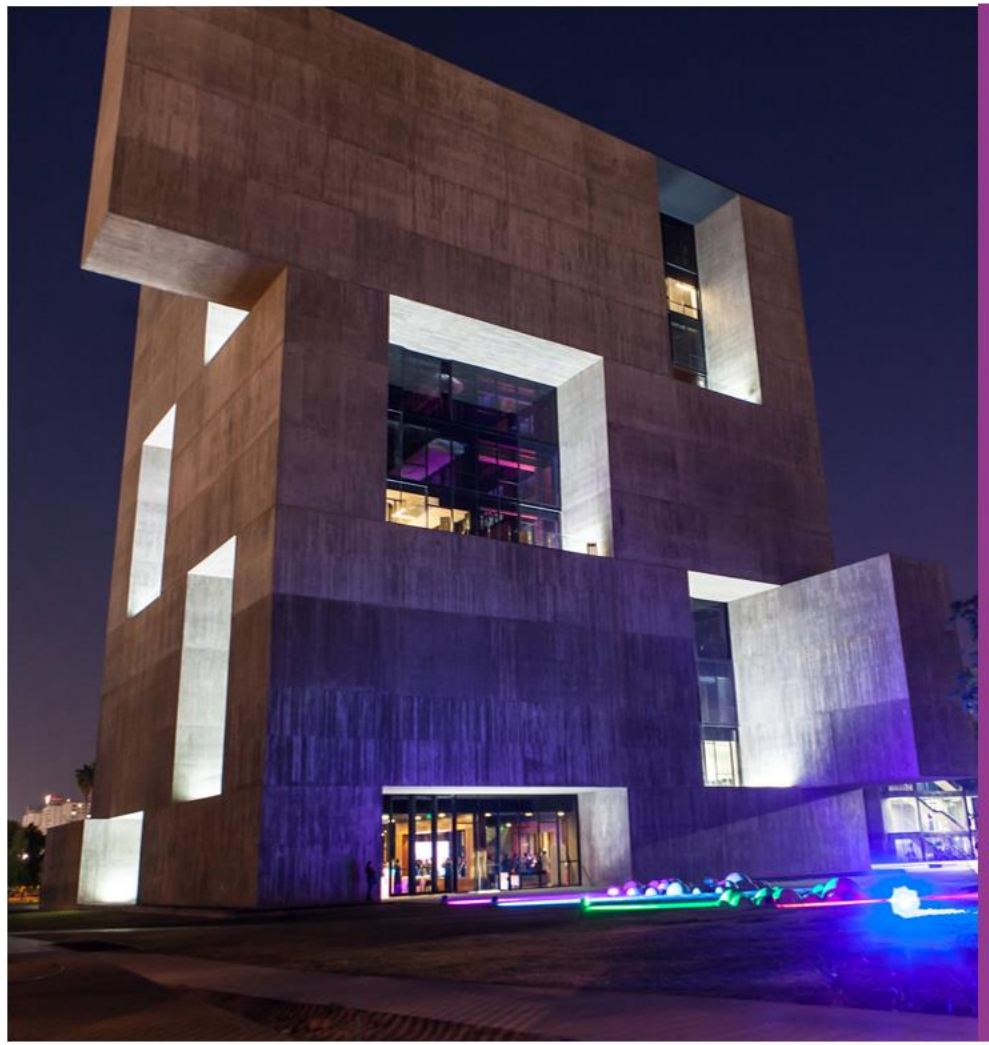
CENTRO DE INNOVACION UC
ANACLETO ANGELINI

CIBERLAB

LABORATORIO DE CIBERDEFENSA PARA LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

"EJERCICIOS DE CRISIS": DETECCIÓN, CONTENCIÓN COMUNICACIÓN, RECUPERACIÓN Y LECCIONES APRENDIDAS

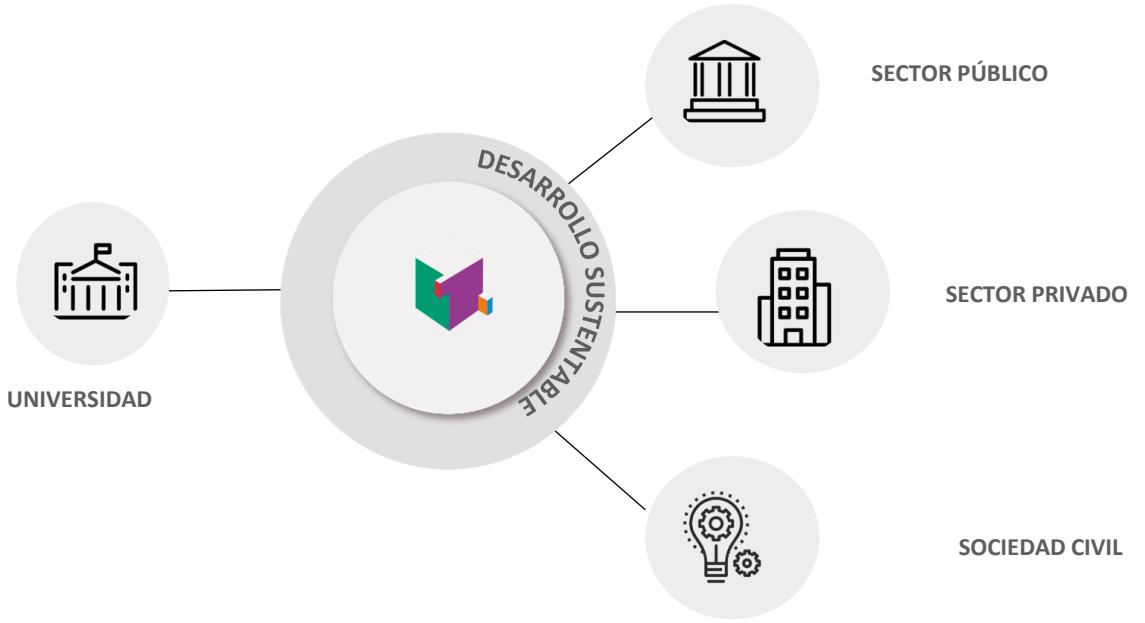
Rocío Ortiz M.
Directora Ejecutiva CIBERLAB
Subdirectora de Industrias del Futuro
Centro de Innovación UC
rortiz@uc.cl



Ecosistema de **Innovación & Emprendimiento**

El Centro de Innovación UC promueve una cultura y un entorno pro innovación y emprendimiento en la Universidad, en el país y la región, a través de encuentros, construcción de redes y la promoción de proyectos conjuntos entre la academia, el sector privado y el sector público.

CONECTANDO A LA UC CON EL ECOSISTEMA DE INNOVACIÓN



El Centro de Innovación UC establece una nueva cuádruple hélice donde la Universidad, el sector público, el sector privado y la sociedad civil se encuentran con el propósito común de llevar a Chile y América Latina hacia una Sociedad del Conocimiento en un mundo globalizado. Fomentando así una mayor inversión en innovación en el país y acercándonos a los países desarrollados.

¿ CÓMO SE CRUZA LA INNOVACIÓN CON LA CIBERSEGURIDAD?

R. Ortiz. 140825

DEFINICIONES Y ALCANCE

DEFINICIÓN " DE MANUAL"

Ciberseguridad entendida como un **proceso integral sistemático** que permite mantener la **confidencialidad, integridad y disponibilidad de la información** (y su infraestructura asociada) en sus etapas de almacenamiento, procesamiento y transferencia, por medio de **políticas, entrenamiento, concientización y tecnología.**

DEFINICIONES Y ALCANCE

DEFINICIÓN " DE MANUAL"

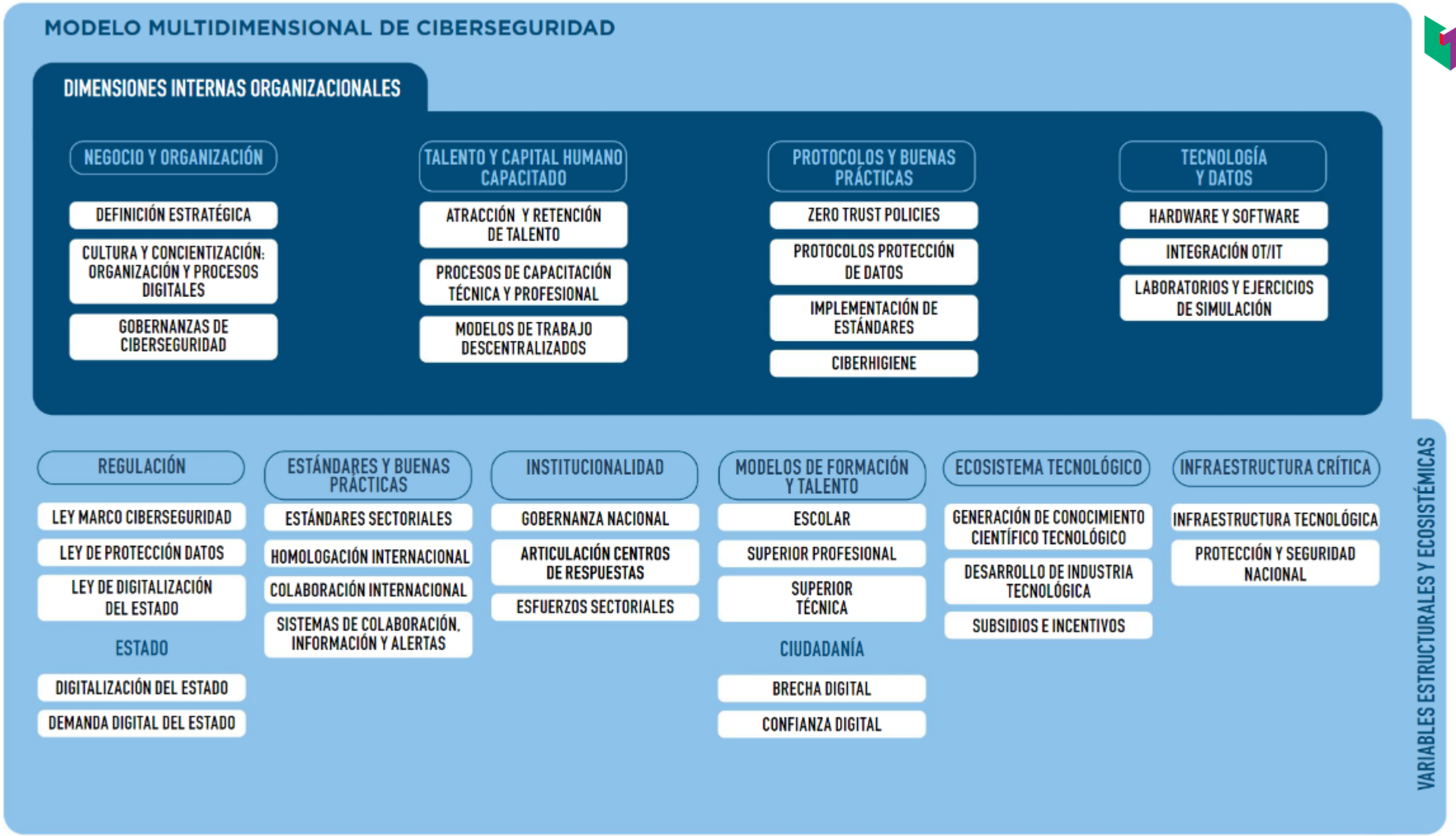
Ciberseguridad entendida como un proceso integral sistemático que permite mantener la confidencialidad, integridad y disponibilidad de la información (y su infraestructura asociada) en sus etapas de almacenamiento, procesamiento y transferencia, por medio de políticas, entrenamiento, concientización y tecnología.

DEFINICIÓN "ECOSISTÉMICA": MÁS ALLÁ DE LO TÉCNICO

- La importancia de la información como **activo estratégico** habilitador de la **toma de decisiones de negocios y de política pública basada en datos** para el **crecimiento económico y bienestar del país.**
- Importancia de la generación de una **confianza digital** ciudadana
- Rol de la **ciberdefensa y el cuidado de las infraestructuras críticas.**
- Oportunidad estratégica de posicionar a Chile como ***Hub*** **regional de ciberseguridad**
- **Prioridad de trabajo a nivel táctico y ejecutivo**

Fuente imagen: Elaboración propia equipo Hoja de Ruta de Ciberseguridad 2022

Modelo de taxonomía vigente al 2025



Fuente imagen: Elaboración propia equipo Hoja de Ruta de Ciberseguridad 2022

Modelo de taxonomía vigente al 2025

CULTURA EN CIBERSEGURIDAD

Desarrollo de mecanismos de adopción de buenas prácticas y ciberhigiene en ciberseguridad, permeando la cultura y el comportamiento organizacional. Esto contempla, tanto a nivel de directorios como a nivel de colaboradores. Así mismo, se considera la cultura en ciberseguridad de usuarios y ciudadanía.

R. Ortiz. 140825

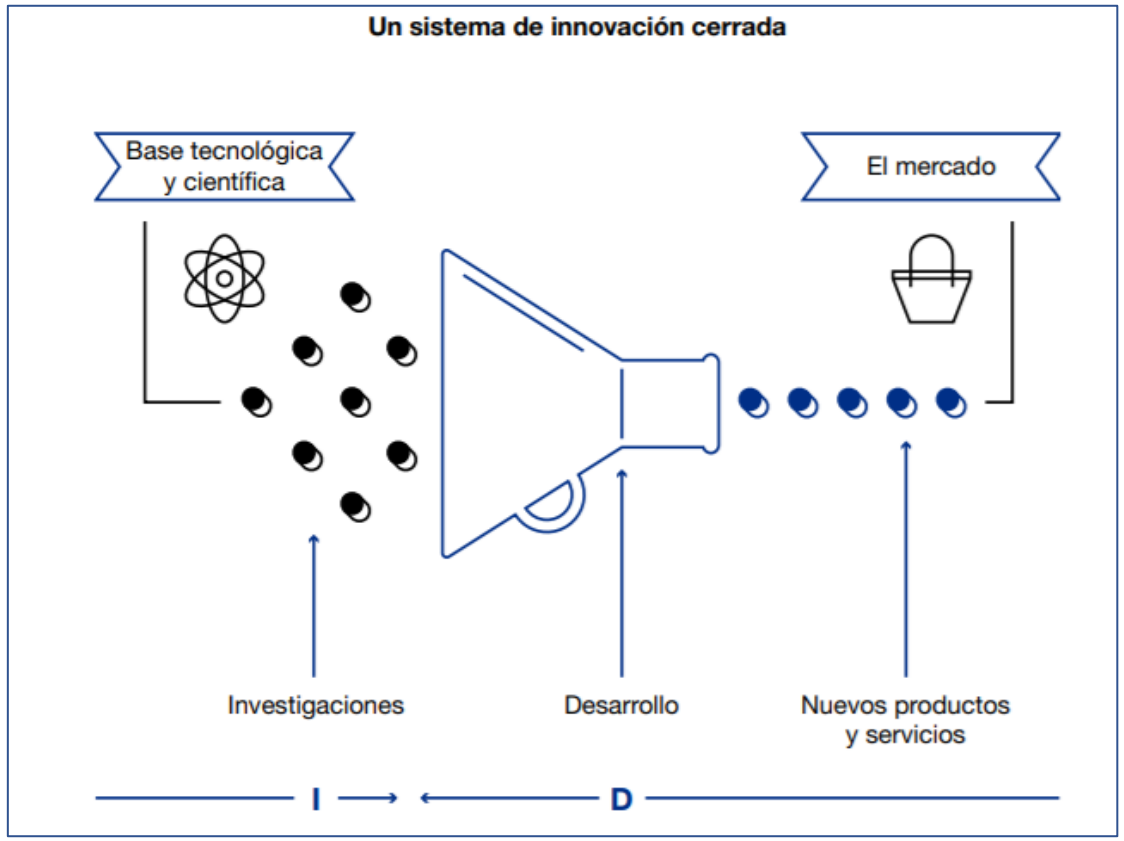
TALENTO Y DESARROLLO DE COMPETENCIAS EN CIBERSEGURIDAD

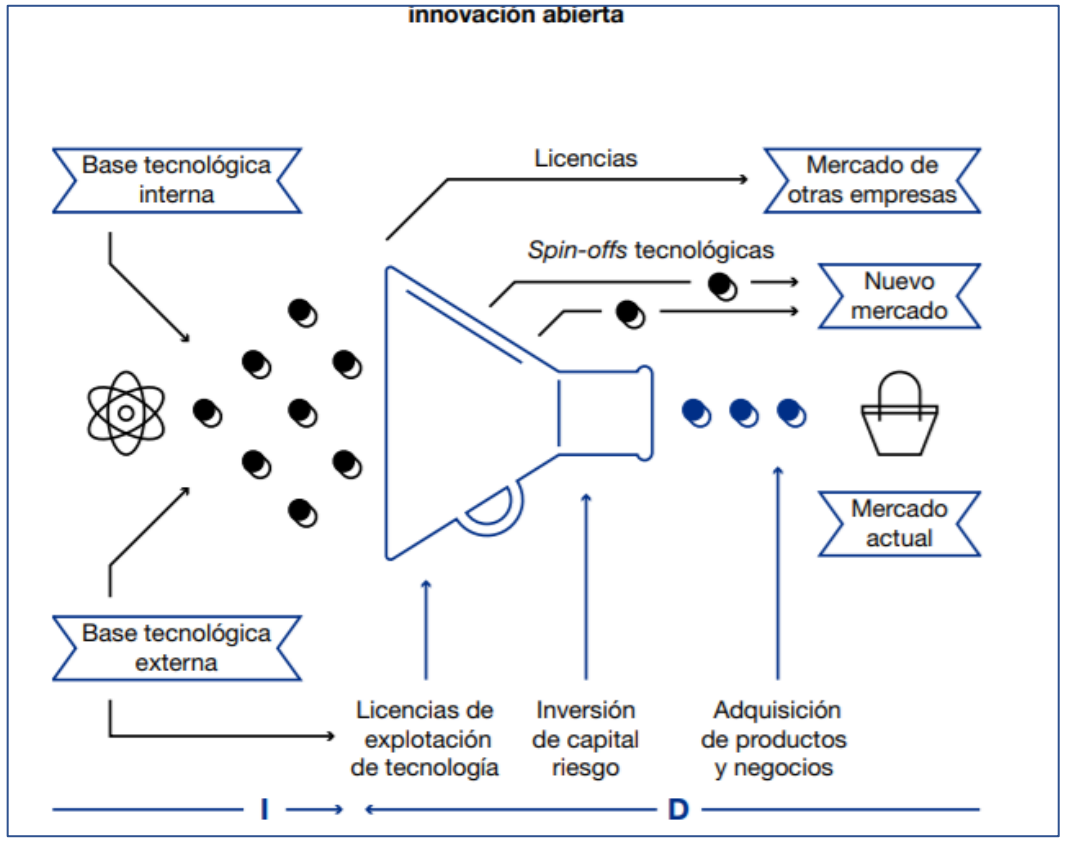
Contempla los desafíos de formación de **talento y competencias para la ciberseguridad**, considerando nuevos modelos educativos desde la formación básica, técnica, profesional hasta la reconversión laboral por medio de la capacitación y certificación no-tradicional de competencias.

TECNOLOGÍA, PROTOCOLOS Y ESTÁNDARES

Implementación y desarrollo de tecnología habilitante para las estrategias de ciberseguridad y la mejora de procesos internos y de negocios. Uso de tecnología y la creación de ecosistemas tecnológicos, así como la implementación de protocolos y estándares que van de la mano de la implementación tecnológica.

LA INNOVACIÓN ABIERTA





VALOR EN LA INTERACCIÓN Y FLUJO DEL ECOSISTEMA

Chesbrough, H. (2019). Open Innovation Results . OUP Oxford.


SIEMENS
Revolucionando la industria
Claro
Contigo en la evolu
R. Ortiz. 140825

"UN PROYECTO *TRIPLE HÉLICE*, PARA CONECTAR Y PROTEGER ACADEMIA, INDUSTRIA Y SECTOR PÚBLICO."

R. Ortiz. 140825

CONTEXTO DE LA COLABORACIÓN ACADÉMICA-MILITAR

El objetivo general del convenio es compartir capacidades, conocimiento y talento con el fin de promover la investigación, transferencia tecnológica y formación. Algunos mecanismos:

- **Intercambio de información, conocimientos, experiencias y apoyo técnico**
- Uso de instalaciones para actividades conjuntas
- Participación conjunta en seminarios y eventos
- **Acciones conjuntas en el área de educación militar**
- Programas de intercambio profesional, estudiantil o técnico
- **Fomento de la investigación y desarrollo**

CIBERLAB

MIEMBROS FUNDADORES

REPRESENTANTES SECTOR PRIVADO Y TECNOLÓGICO

aws
DREAMLAB TECHNOLOGIES
Claro empresas
LAB X2X
TECNOLOGÍAS EMERGENTES PARA LA CONECTIVIDAD DEL FUTURO
paloalto NETWORKS
Scitum
SIEMENS
THALES
Building a future we can all trust

REPRESENTANTES INFRAESTRUCTURAS CRÍTICAS

COORDINADOR ELÉCTRICO NACIONAL
banca asociación de bancos
CCMIN CORPORACIÓN DE CIBERSEGURIDAD MINERA
conecta logística

REPRESENTANTES SECTOR PÚBLICO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

REPRESENTANTES SECTOR DEFENSA Y SEGURIDAD

EJÉRCITO DE CHILE

REPRESENTANTES ACADEMIA

dictuc CETIUC
DuocUC
FACULTAD DE DERECHO PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
DERECHO, CIENCIA Y TECNOLOGÍA UC

R. Ortiz. 140825

COMITÉ TECNOLÓGICO E I+D+i

COMITÉ DE CAPITAL HUMANO Y DESARROLLO DE COMPETENCIAS

COMITÉ DE *ADVOCACY* Y *PUBLIC POLICY*

CIBERLAB

DESAFÍOS Y BRECHAS

*"Un **espacio asociativo neutral** para abordar los desafíos de ciberseguridad y ciberdefensa de las infraestructuras críticas del país"*

- Nuevas demandas ante la **Ley Marco de Ciberseguridad.**
- **Formación de competencias de carácter práctico,** de forma flexible, constante, actualizada y personalizada.
- **Desarrollo de *sandboxes* y espacios de pilotaje.**
- **Modelos de asociatividad con otros actores del ecosistema,** que permitan compartir experiencias y aprendizajes actualizados.

R. Ortiz. 140825

ESTRUCTURA Y LÍNEAS DE ACCIÓN

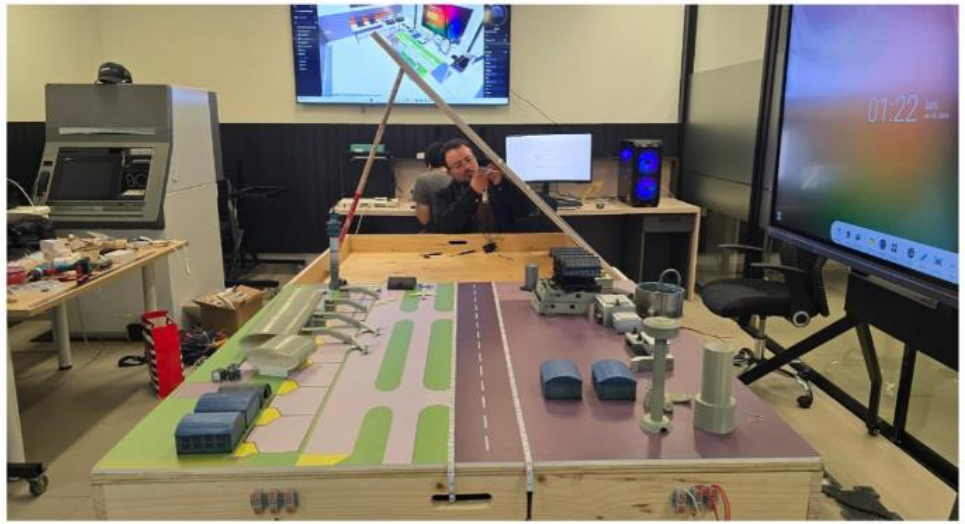
Fuente imagen: Reporte de Impacto 2024-2025 Ciberlab

CIBERLAB

ESPACIO FÍSICO E INFRAESTRUCTURA

- Instalaciones físicas avanzadas y colaborativa.
- Sandboxes y laboratorios especializados
- Infraestructura digital y plataforma tecnológica compartida
- Apoyo para I+D+i y pilotos tecnológicos

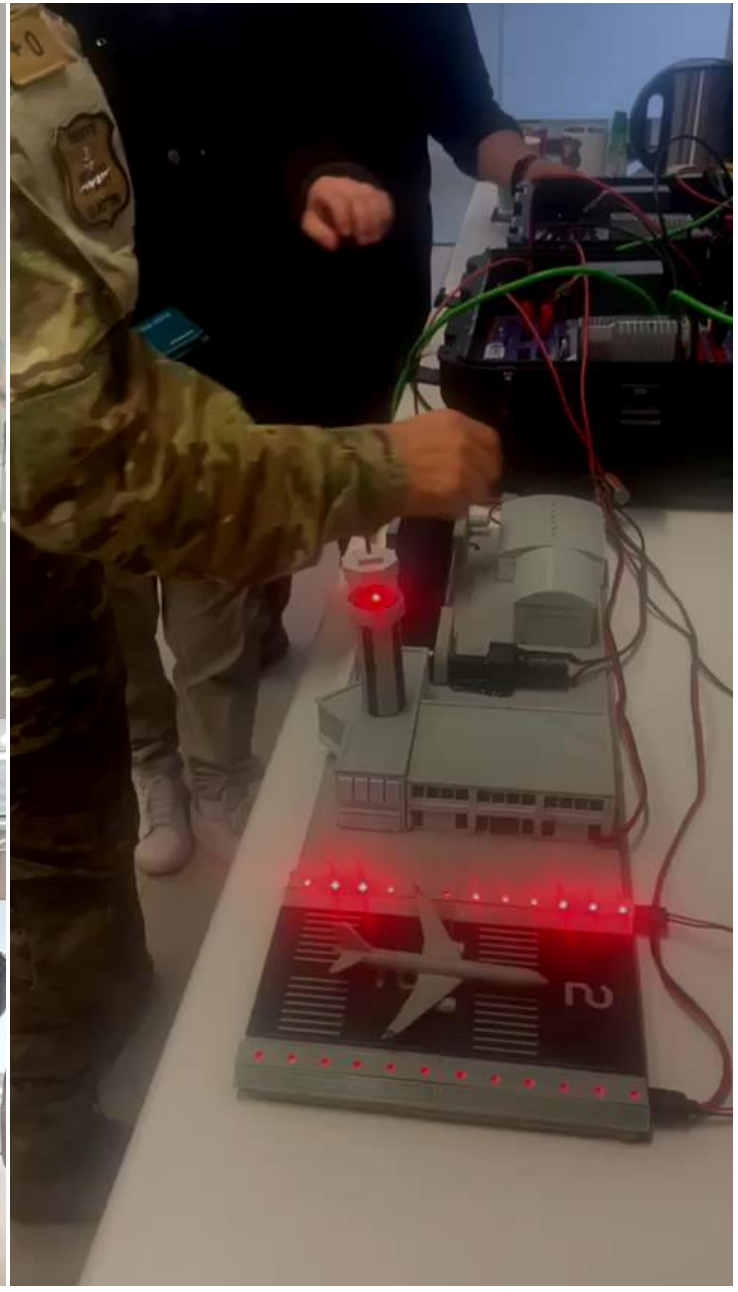
Centro de Innovación y Transferencia Tecnológica Duoc UC en Concepción.

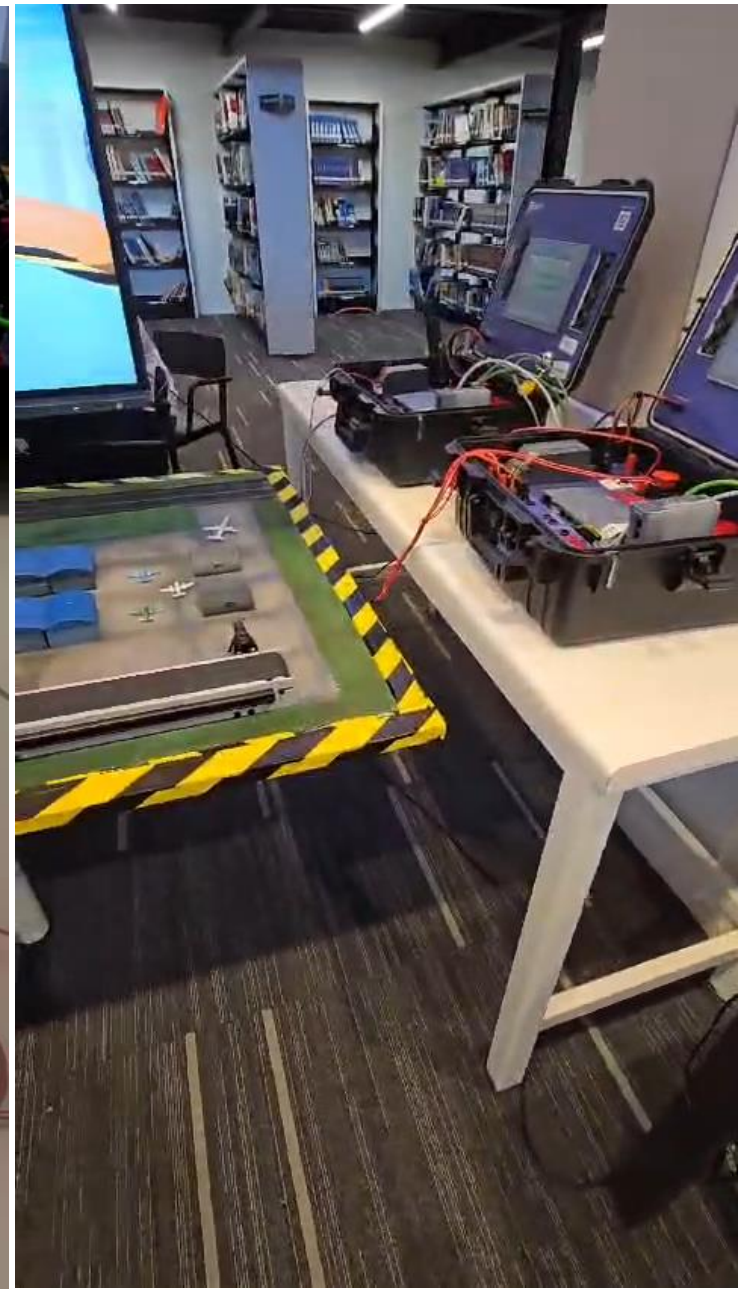


Desarrollo de maqueta simuladores CTF.

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

Fuente imagen: Reporte de Impacto 2024-2025 Ciberlab





CIBERLAB

ALGUNAS CIFRAS

INAUGURACIÓN: 30 DE JULIO 2024

17 miembros fundadores

CAPACIDADES Y DIFUSIÓN

- **3** Programas formativos en curso
- **+320** personas en proceso de capacitación
- **2** seminarios CIBERLAB organizados
- **1** ejercicio gestión crisis
- **+8** Talleres técnicos ejecutados y/o programados

- ✓ **+1000** participantes en actividades y ejercicios
- ✓ Invitaciones a participar en encuentros y eventos de alta convocatoria.
- ✓ **+20** visitas técnicas y comitivas
- ✓ Alta presencia medios masivos de comunicación, relevando la importancia de la temática.

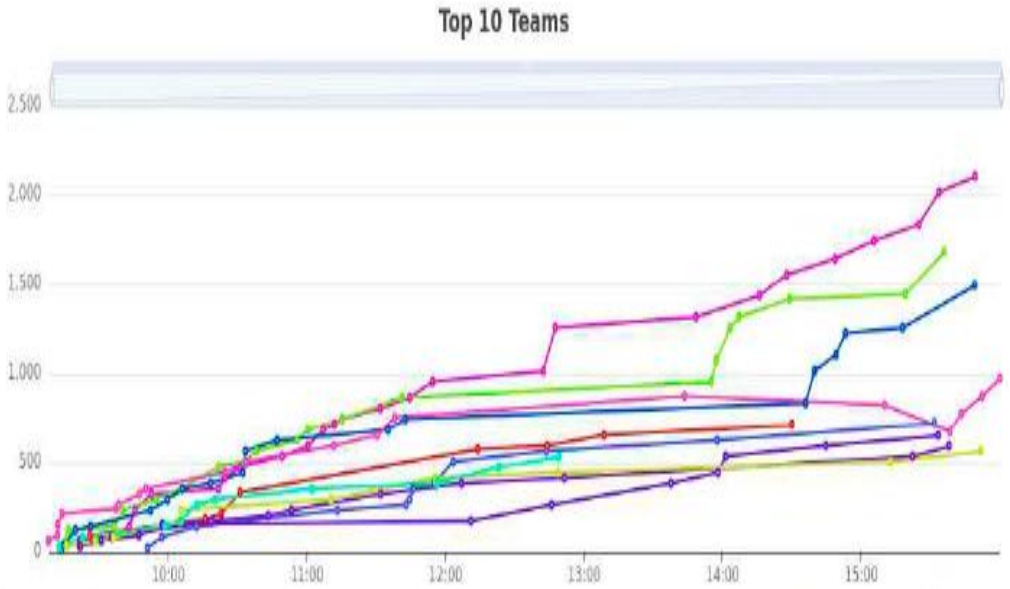
PILOTOS

- **1** Plataforma IdC
- **+ 8** Pilotos y pruebas de concepto
- **2** maqueta/simuladores
- **+30** estudiantes y tesistas
- **+15** académicos e investigadores
- **+7** disciplinas

CIBERLAB

CTF LLAITÚN 2024

El ejercicio de ciberdefensa combina 10 desafíos estilo CTF y 4 escenarios de infraestructura crítica simulada. Los desafíos CTF incluyen actividades como análisis de malware, exfiltración de datos, escalada de privilegios, inyección SQL, y pentesting, entre otros.
Desarrollado junto al Ejército de Chile, Dreamlab Technologies y DUOC




ACADEMIA POLITECNICA MILITAR

CIBERLAB

EJERCICIOS Y SIMULACIONES GESTIÓN DE CRISIS

- El equipo del Ciberlab- perteneciente al Centro de Innovación UC y el Ejército de Chile, junto a DreamLab Technologies LATAM, el Programa de Derecho, Ciencia y Tecnología de la UC y Duoc UC, convocaron al **primer ejercicio de simulación de un ciberataque,** permitiéndole a los asistentes adquirir competencias para gestión de crisis y levantamiento de buenas prácticas.

+120 participantes

CIBERLAB

EJEMPLOS PERFILES PARTICIPANTES

Los participantes representan a los involucrados en los protocolos de comité de crisis o equivalente de la organización. De no existir una definición, se sugieren al menos los siguientes roles:

ALTA DIRECCIÓN Y TOMADORES DE DECISIONES

- Tomadores de decisiones estratégicos, como gerentes generales o directivos de organizaciones de áreas críticas.
- Rol: Evaluar riesgos globales, tomar decisiones estratégicas y supervisar la implementación de acciones.

EQUIPOS TÉCNICOS DE SEGURIDAD

- Gerentes y equipos de ciberseguridad, analistas de SOC, administradores de sistemas y redes.
- Rol: Definir el plan técnico e identificar, contener y mitigar ciberamenazas durante el ejercicio.

EQUIPOS DE COMUNICACIÓN

- Representantes de relaciones públicas, voceros y encargados de comunicación interna y externa.
- Rol: Manejar mensajes hacia la prensa, *stakeholders* y equipos internos durante y después de la crisis.

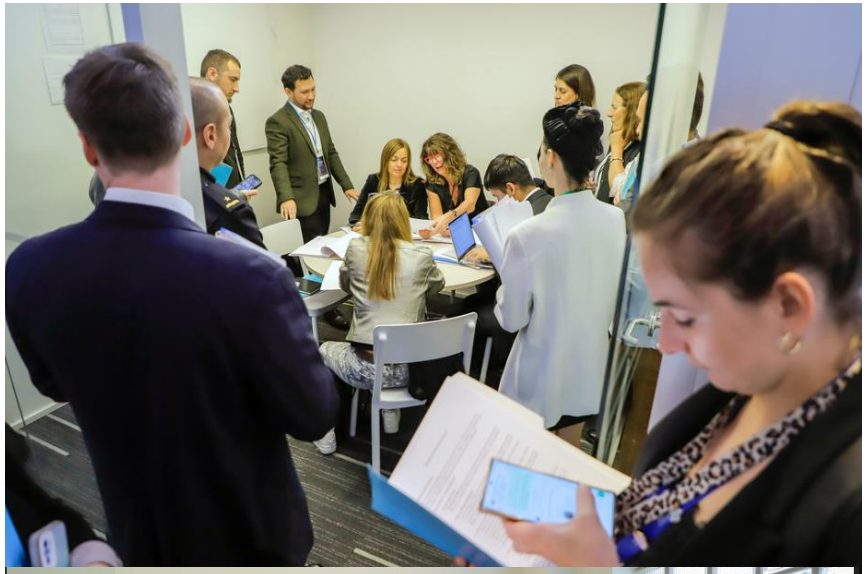
EQUIPOS LEGALES Y DE CUMPLIMIENTO

- Abogados especialistas en ciberseguridad, derecho tecnológico, privacidad de datos y cumplimiento normativo.
- Rol: Identificar posibles responsabilidades legales durante un incidente real y evaluar riesgos legales asociados a las respuestas planteadas en el ejercicio.

El análisis y reporte se centrará en estas 4 dimensiones de análisis.

CIBERLAB

SIMULACIÓN ESCENARIO DE CRISIS



CONTENIDO

Simulación práctica de un escenario de crisis provocado por ciberataque, donde los participantes deberán responder utilizando el marco NIST* o equivalente y/o normativa/ estándar vigente para la empresa/industria.

OBJETIVO GENERAL

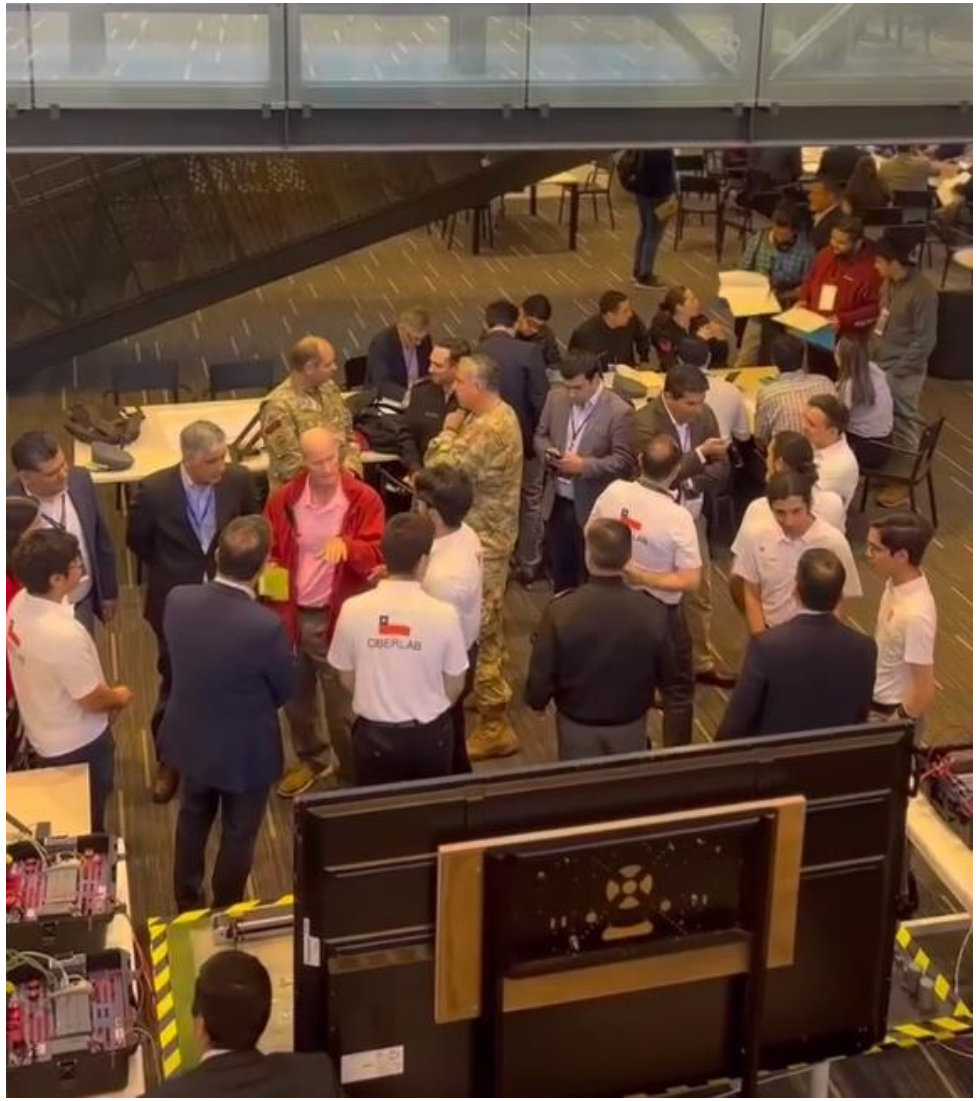
Facilitar el desarrollo de ejercicios integrados de simulación para la gestión de crisis cibernéticas, enfocados en fortalecer la preparación, la coordinación y la toma de decisiones estratégicas para proteger infraestructuras críticas frente a ciberataques.

CIBERLAB

PARTICIPACIÓN PÚBLICO, PRIVADO Y ACADÉMICA

OBJETIVOS ESPECÍFICOS

- Desarrollar resiliencia organizacional
- Fortalecer la coordinación interinstitucional, Promover la adopción de buenas prácticas en ciberseguridad
- Evaluar la capacidad de reacción y recuperación
- Fomentar la comunicación estratégica



CIBERLAB

APRENDIZAJES

- **Importancia de la coordinación inter-áreas:**
  - La participación de **alta dirección**, **equipos técnicos**, **comunicación** y **área legal** demuestra que la gestión de crisis no es solo un tema técnico, sino que requiere decisiones estratégicas, manejo comunicacional y control del riesgo legal.

- **Valor del enfoque asociativo y multiactor:**
  - Reunir actores de distintas áreas y organizaciones (pública-privada-académica) potencia la visión global del riesgo y permite aprender de otras experiencias.

  - Genera confianza y canales de colaboración que pueden ser útiles en incidentes reales.

CIBERLAB

APRENDIZAJES

- **Fortalecimiento de la comunicación interna y externa:**
  - Se evidencia la necesidad de flujos de información claros hacia la prensa, stakeholders y personal interno, evitando mensajes contradictorios o tardíos.
  - Se refuerza la importancia de entrenar voceros.
  - Protocolos de comunicación interna aún requieren más rapidez y estandarización para evitar información fragmentada entre áreas.

CIBERLAB

ACCIONES RECOMENDADAS

- Actualizar el plan de gestión de crisis incorporando ajustes a roles, flujos de información y niveles de autoridad.
- Realizar entrenamientos cruzados entre áreas técnicas, legales, comunicacionales y directivas para aumentar comprensión mutua.
- Establecer métricas de desempeño para evaluar rapidez de respuesta, claridad comunicacional y efectividad técnica.
- ***Planificar ejercicios combinados con incidentes técnicos, de reputación y regulatorios para aumentar resiliencia organizacional.***

d) Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y sistemas para detectar acciones o programas informáticos que comprometan la ciberseguridad y comunicar la información relativa a dichas acciones o programas al CSIRT Nacional, en la forma que determine el reglamento.

y) Coordinar anualmente, durante el mes de octubre, un ejercicio nacional de comprobación de capacidades de ciberseguridad, en cumplimiento de la ley N° 21.113, que declara el mes de octubre como el mes nacional de la ciberseguridad.

CIBERLAB

COMPETENCIAS ADQUIRIDAS

Existen competencias específicas para cada rol y competencias transversales:

ALTA DIRECCIÓN Y TOMADORES DE DECISIONES

- Toma de decisiones bajo presión.
- Visión global del riesgo.
- Priorización y asignación de recursos.

EQUIPOS TÉCNICOS DE SEGURIDAD

- Detección y análisis de incidentes.
- Contención y mitigación.
- Uso coordinado de herramientas y plataformas de ciberinteligencia.

EQUIPOS DE COMUNICACIÓN

- Manejo de comunicación interna y externa en crisis.
- Relación con medios y stakeholders.
- Gestión de flujos de información.

EQUIPOS LEGALES Y DE CUMPLIMIENTO

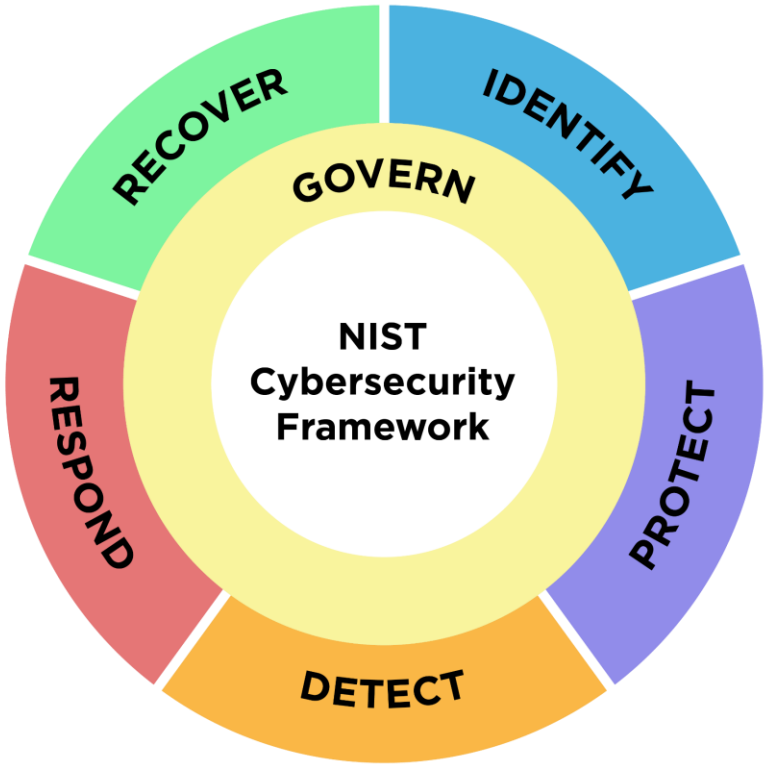
- Identificación de riesgos legales
- Aplicación de marcos legales y de privacidad de datos
- Integración de criterios legales en la estrategia de mitigación.

COMPETENCIAS TRANSVERSALES DE COORDINACIÓN Y COLABORACIÓN

¿GESTIÓN DE CRISIS? ¿GESTIÓN DE INCIEDENTES? ¿CONTINUIDAD OPERACIONAL?

CIBERLAB

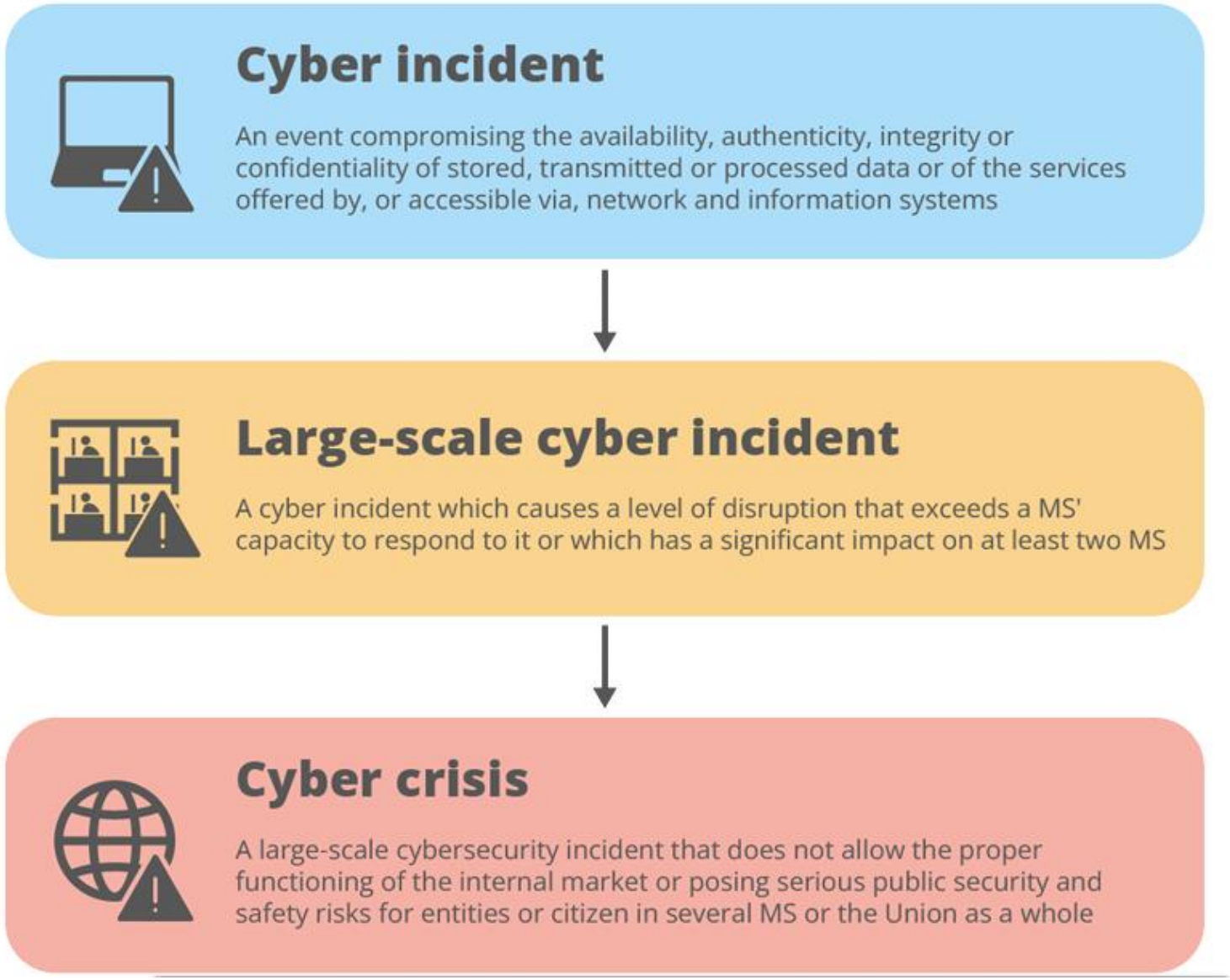
MARCO GENERAL NIST Y CICLO DE VIDA DE LA GESTIÓN DE CRISIS



Fuente imagen: https://www.nist.gov/image/nist-cybersecurity-framework-20

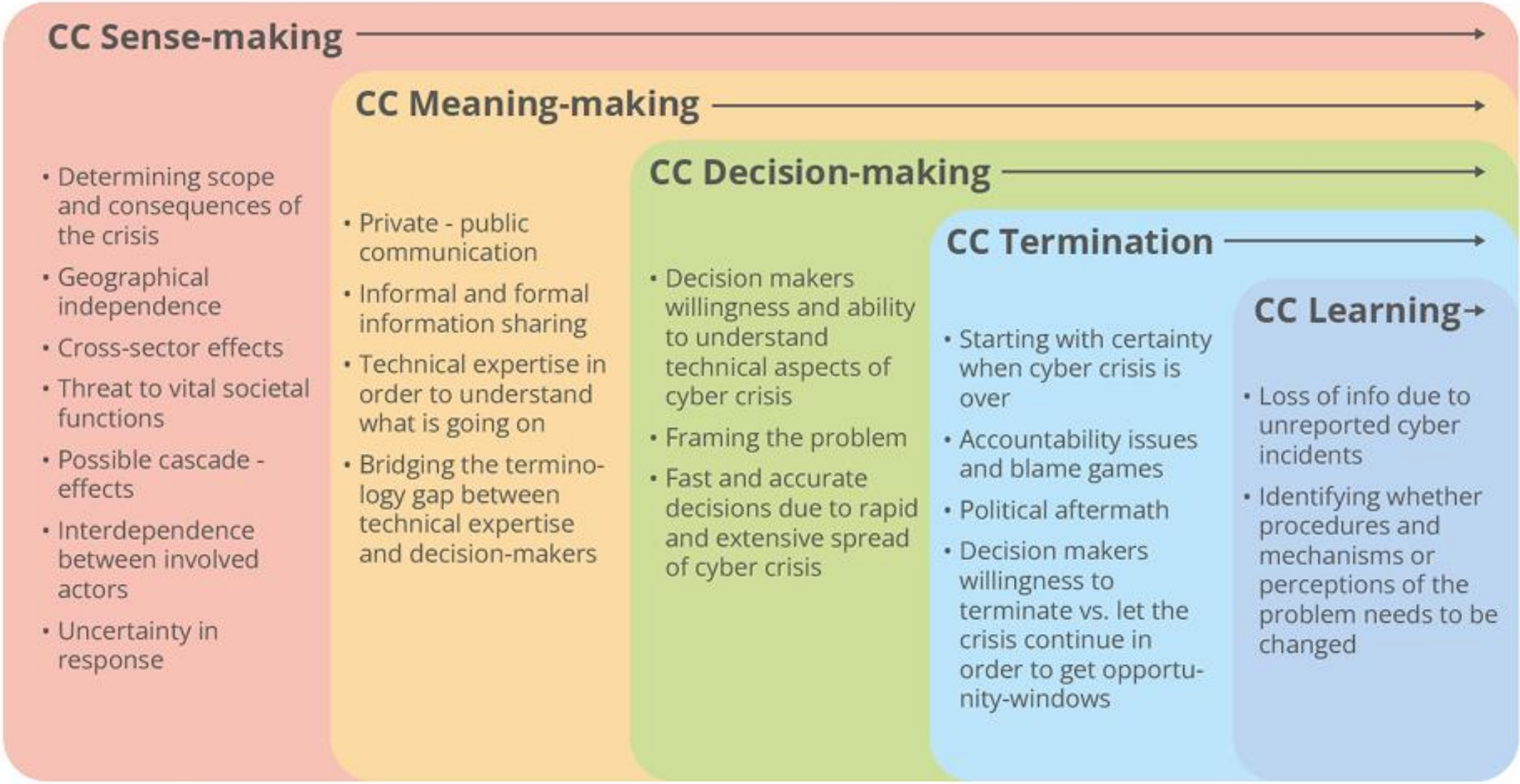
Fuente imagen: https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

DE GESTIÓN DE INCIDENTES A GESTIÓN DE CRISIS



Fuente imagen: https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

DE GESTIÓN DE INCIDENTES A GESTIÓN DE CRISIS



Fuente imagen: https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

CIBERLAB

¿CUÁNTOS PLANES SE NECESITAN ?

TIPO DE PLAN	ALCANCE	FRAMEWORKS/PLAYBOOKS
✓ *Business Continuity Plan (BCP)*	• Operaciones transversales	• ISO 22301, NFPA 1600, NIST CSF, COBIT, UNDP BCM
✓ *Disaster Recovery Plan (DRP)*	• Recuperación TI	• ISO 22301, NIST SP 800-34, ISO/IEC 27031
✓ *Incident Response Plan (IRP)*	• Respuesta de incidente de Ciberseguridad	• NIST SP 800-61, ISO/IEC 27035, SANS
✓ *Crisis Management Plan (CMP)*	• Coordinación ejecutiva	• ENISA Best Practices, ISO 22361, NIS2
✓ *Cyber Crisis Mgmt Playbook*	• Operación de crisis de ciberseguridad	• ENISA, CISA Playbooks, NIST CSF, SOC Playbooks
✓ *Ransomware BCP/DRP u otro*	• Específico al tipo de ataque	• CISA, NCSC UK, ISO 22301-based, Sectoral Guides
✓ *Emergency Communication Plan*	• Comunicación de Crisis	• ISO 22301, ENISA, National Guidance

Fuente imagen: Elaboración propia

¿CUÁNTOS PLANES SE NECESITAN ?

Fuente imagen: https://blog.bcm-institute.org/cyber-security/bcm-cir-concepts-related-bcm-concepts-to-cyber-security

CIBERLAB

ESPACIO DE DIFUSIÓN DE CONOCIMIENTO

- Encuentro enfocado en una discusión sobre la colaboración pública, privada y académica y el uso de tecnologías para la ciberseguridad con foco en la protección de infraestructuras e industrias críticas.

¿ QUÉ QUEREMOS A FUTURO?

- ✓ AUMENTAR EL IMPACTO Y ALCANCE
- ✓ DUPLICAR LOS RESULTADOS IMPACTADOS ESTE AÑO
- ✓ EMPUJAR NUEVAS LÍNEAS DE TRABAJO JUNTO A NUEVOS *PARTNERS* NACIONALES E INTERNACIONALES
- ✓ AMPLIAR Y DIVERSIFICAR LA BASE DE TALENTO NACIONAL E INTERNACIONAL

LA COLABORACIÓN DE LA TRIPLE HÉLICE ES FUNDAMENTAL PARA ROBUSTECER LAS CAPACIDADES DEL ECOSISTEMA Y DESARROLLAR RESILIENCIA CIBERNÉTICA A NIVEL REGIONAL, NUESTRA MEJOR DEFENSA ES FORTALECER ESTOS ESPACIOS ASOCIATIVOS.

CENTRO DE INNOVACION UC
ANACLETO ANGELINI

CIBERLAB

LABORATORIO CIBERDEFENSA PARA LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Rocío Ortiz M.
Subdirectora de Industrias del Futuro
Centro de Innovación UC
rortiz@uc.cl
ciberlab.uc.cl