Foro Nacional
de Ciberseguridad

CONSOLIDADO INFORMES DE TRABAJO

FORO NACIONAL DE CIBERSEGURIDAD

DICIEMBRE 2024

ÍNDICE

DIMENSIÓN 1:

Política y Estrategia Nacional de Ciberseguridad

Moderadores:

Marcos Soto Briones
Francesca Gatica Aliaga

Participantes de la Dimensión

Los participantes en la creación, diseño y gestión del presente documento de la dimensión fueron los siguientes:

1. Jorge Carrasco Cabrales.
2. Marcos Soto Briones.
3. Marcelo Pérez Rodríguez.
4. Marcelo Rodriguez Kong.
5. Rodrigo Testón Nahuelhuil.
6. Daniel Escobar Rodriguez.
7. Doris Herrera.
8. Natan Finol Bencomo.
9. Pablo Fabres.
10. Mario Urriola.
11. Alejandro Mellado.
12. Raúl Ceballos Fuentes.
13. Jimmy Ríos.
14. Daryl Zavala Guerrero.
15. Cristian Flores Cotal.
16. Emilio Muñoz Silva.
17. Andrés Cardenas.
18. Favio Contreras.
19. Camilo Flores.
20. Francesca Gatica Aliaga.

Agradecer también a los participantes que estuvieron colaborando en los diferentes foros de discusión publicados en el sitio web.

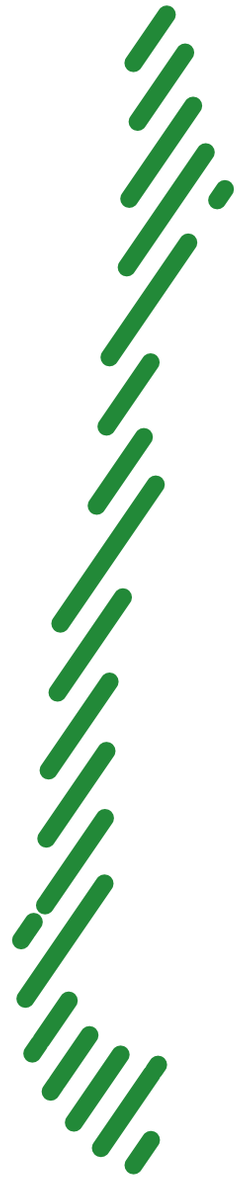
→ RESUMEN

En la actualidad Chile continúa avanzando en el desarrollo de ciberseguridad, que incluye promulgación y/o actualización de leyes y con ello, las obligaciones legales. Dentro de este aspecto los medios juegan una alta importancia y es ahí donde nuestra participación y aporte en la Dimensión de Política y Estrategia Nacional de Ciberseguridad toma una relevancia importante, ya que pretende orientar a todo tipo de organización en su estrategia de Ciberseguridad. La vanguardia de tecnologías sobre ciberseguridad tiene costos bastante altos, donde no todas las organizaciones tienen la capacidad de acceder a ellas, sin embargo, acortar la brecha es imperativo para fomentar su desarrollo.

Actualmente en nuestro país, gracias a procesos de avance sostenido y, acorde a las iniciativas innovadoras que tuvieron su génesis y, materializadas en políticas públicas emanadas desde el Senado de la República, comprendieron la necesidad en el desarrollo y gestión de canalizar inquietudes y fomentar el trabajo colaborativo y, en equipo de expertos de variadas industrias y de la sociedad civil, para enfrentar el desafío impuesto en aras de la protección de nuestra sociedad, enfocando los esfuerzos en la protección de la seguridad en línea, los derechos digitales y, las necesarias soluciones para robustecer la Política y Estrategia Nacional de Ciberseguridad, ofreciendo transformar los desafíos, en ventajas competitivas y estratégicas, permitiendo a las organizaciones de todo tipo contar con herramientas que maximicen la eficacia y fomenten la flexibilidad en un escenario de constante evolución.

Asimismo, considerado el grado de desarrollo tecnológico presente en las industrias a nivel global, las cuales, ofrecen productos y servicios en sus respectivas áreas sectoriales, ha permitido acercar a las personas, comunidades y organizaciones, a activos de valor que mejoran su bienestar, flexibilizan procesos productivos y optimizan la eficacia en la toma de decisiones estratégicas, a todo nivel. Desde encender un interruptor eléctrico, hasta el monitoreo en tiempo real de mercancías que se mueven por todo tipo de medios; la digitalización de procesos en las áreas público y privadas, desde las pymes hasta la salud, el desafío del transporte en todas sus modalidades e industrias, desde cordillera a mar; la industria de la minería, la banca, el retail, y asimismo, otros servicios esenciales como el área de la defensa, infraestructuras críticas, hasta redes sociales; en fin, multiplicidad de organizaciones y dimensiones diversas, actuando e interactuando en un universo atomizado de intereses colectivos como individuales, moviéndose vertiginosamente a través de plataformas de servicios digitales que, no son ajenas a los desafíos de la ciberseguridad.

Por otra parte, el desarrollo de los objetivos definidos en el grupo de trabajo de la Dimensión 1, Política y estrategia de Seguridad Cibernética, consideraron la construcción de una estrategia nacional para asegurar la protección de la infraestructura crítica considerando procesos integrales de respuesta ante incidentes; El establecimiento y gestión de actividades de protección, para garantizar la continuidad, disponibilidad e integridad de los activos y el debido resguardo a la continuidad del negocio para, finalmente, materializar un Plan de Defensa de Ciberseguridad que resguarde a la ciudadanía, los activos y a la infraestructura a nivel nacional, en los ámbitos público-privados. Finalmente, agradecer el esfuerzo y dedicación a todos los desinteresad@s profesionales que aportaron desde cada área: de la academia, industrias de servicios esenciales, instituciones público-privadas, el interés personal proyectado desde la sociedad civil, en fin, dedicar éstas últimas líneas para destacar este esfuerzo mancomunado durante todas aquellas jornadas de análisis, levantamiento de brechas y comprensión de datos, experiencias técnicas, revisión de *frameworks* y literatura necesaria para avanzar en el propósito encomendado, donde voluntariamente la motivación de proteger a Chile en la dimensión digital y tecnológica, permitirá ofrecer este documento que aporte con un grano de arena al crecimiento sostenido de las políticas de protección de seguridad de la información en la mayor cantidad de lugares de nuestra querida Patria.



→INTRODUCCIÓN

El Foro Nacional de Ciberseguridad es una iniciativa de innovación en generación de políticas públicas al alero del Senado y con la participación a *long way to the top* de expert@s, que permitirá canalizar inquietudes y fomentar la colaboración en el ámbito de la ciberseguridad en Chile. Este foro se convierte en un espacio donde expert@s se reúnen para discutir ideas, compartir conocimientos y promover medidas que fortalezcan nuestra seguridad digital. El Foro Nacional de Ciberseguridad es un espacio que invita a académicos, profesionales, empresas y organizaciones interesados en la ciberseguridad a unirse a nuestro esfuerzo. Juntos, podemos fortalecer la seguridad en línea, proteger los derechos digitales y promover un ciberespacio confiable y generar soluciones.

→Principios rectores de la Política Nacional de Ciberseguridad

Considerando que en la actualidad las actividades humanas en múltiples dimensiones están gobernadas por el entorno digital, la Política Nacional de Ciberseguridad debe estar centrada en la protección de los ciudadanos. Es fundamental garantizar la seguridad de las personas mediante la protección de la infraestructura crítica, los datos personales y la soberanía tecnológica del país. Para lograrlo, se hace necesario definir los principios rectores que permitirán canalizar la política y definir las estrategias adecuadas. Estos principios son los siguientes:

I. Protección Integral y Proactiva por diseño: La ciberseguridad debe considerar a todos los actores de la infraestructura digital del país, desde los sistemas gubernamentales hasta las organizaciones privadas y los ciudadanos. Este principio destaca que la seguridad debe incorporarse desde el inicio del diseño de los sistemas, en lugar de implementarse como una solución posterior. Un enfoque preventivo y estructural permite anticipar y mitigar riesgos antes de que se materialicen. La implementación de seguridad desde el diseño, junto con la vigilancia continua y la detección temprana de amenazas, es esencial para mantener una infraestructura digital segura y resiliente.

II. Responsabilidad multisectorial: La ciberseguridad no es solo una responsabilidad del Estado; involucra tanto al sector público como al privado, además de otros actores clave como la academia y la ciudadanía. Este principio reconoce que, para lograr una ciberseguridad efectiva, es esencial un enfoque colaborativo, en el que cada sector asuma un papel activo en la prevención, gestión y respuesta a incidentes cibernéticos. La cooperación entre los diferentes actores es clave para enfrentar de manera eficaz las amenazas en el entorno digital.

III. Enfoque en la resiliencia: Las amenazas cibernéticas son inevitables, por lo que la política de ciberseguridad debe enfocarse en generar condiciones para favorecer la resiliencia de servicios e infraestructuras física y digitales de interés nacional, asegurando una rápida recuperación ante incidentes. Esto minimiza el impacto de los ataques y garantiza la continuidad de las operaciones esenciales, evitando así interrupciones que afecten a las personas.

IV. Protección de Derechos y Libertades: Este principio busca garantizar que las medidas de ciberseguridad no comprometan los derechos fundamentales de los ciudadanos, como la privacidad y la libertad de expresión. Cualquier acción en materia de ciberseguridad debe respetar los principios de los derechos humanos, asegurando un equilibrio entre la protección de la sociedad y la salvaguardia de las libertades individuales en el entorno digital.

V. Innovación y adaptabilidad: El entorno digital y las amenazas cibernéticas están en constante evolución, lo que exige una política de ciberseguridad flexible y capaz de ajustarse rápidamente a los avances tecnológicos y nuevos riesgos. Este principio impulsa la inversión en tecnologías emergentes y la adopción de prácticas innovadoras, permitiendo al Estado y a las organizaciones anticiparse y responder eficazmente a las amenazas, manteniéndose a la vanguardia en la defensa cibernética.

VI. Transparencia: La confianza es un pilar fundamental en la gestión de la ciberseguridad. Este principio asegura que tanto el gobierno como las organizaciones actúen con transparencia y rindan cuentas sobre sus acciones. Los ciudadanos deben estar informados sobre cómo se protegen sus datos y las medidas que se adoptan ante incidentes, garantizando una comunicación clara y accesible en todo el proceso de gestión de la ciberseguridad.

VII. Colaboración Internacional: La ciberseguridad es un desafío global que requiere cooperación más allá de las fronteras. Este principio destaca la importancia de que Chile participe activamente en foros y acuerdos internacionales que permitan compartir información, responder a amenazas globales de manera coordinada y adoptar estándares internacionales en materia de ciberseguridad sin dejar de lado o a posteriori el interés nacional.

VIII. Soberanía tecnológica: La Política Nacional de Ciberseguridad debe considerar acciones a largo plazo que permitan adquirir mayores niveles de control sobre la tecnología en términos de fabricación, uso y mantenimiento. Este principio subraya que no es posible alcanzar una verdadera ciberseguridad si un país no controla las tecnologías críticas que utiliza. A través de la promoción del desarrollo tecnológico local, la reducción de la dependencia de tecnologías extranjeras y la inversión en capacidades nacionales se busca asegurar que Chile tenga la autonomía necesaria para proteger sus intereses digitales y estratégicos.

IX. Cumplimiento Normativo y Colaboración Interinstitucional: La Política Nacional de Ciberseguridad debe considerar la colaboración y articulación de los esfuerzos públicos para el cumplimiento de las leyes y normas vigentes, explicitando la colaboración en materias de ciberseguridad, entre las instituciones públicas que previenen y combaten los delitos informáticos y el crimen organizado. La colaboración debe ser planteada como una herramienta para fortalecer las capacidades de ciberdefensa de la Nación en cuanto la resiliencia, la respuesta a incidentes, la protección de los ciudadanos y las infraestructuras críticas.

X. Planificación y Gestión de la Ciberdefensa: La Política Nacional de Ciberseguridad debe abordar las líneas estratégicas que permitan a la Nación hacer frente a una crisis provocada por ataques cibernéticos de alta complejidad, que tengan como finalidad interrumpir el funcionamiento de las infraestructuras críticas de la nación, así como también afectar directamente a la integridad de la población. La coordinación de todos los actores y la creación de planes de gestión y respuesta multisectoriales es vital para la prospección de escenarios de riesgos y la preparación de las capacidades de respuesta.

→Problemáticas Detectadas

A nivel mundial, las problemáticas relacionadas con el tratamiento de la ciberseguridad se han complejizado, desarrollando características que todas las organizaciones, tanto públicas como privadas, deben integrar en su estrategia. Los impactos financieros, operacionales y reputacionales derivados de las amenazas cibernéticas podrían llevar a estas organizaciones a situaciones de alta complejidad.

En este contexto, la Política y Estrategia Nacional de Ciberseguridad es fundamental, ya que indicará lineamientos clave sobre cómo abordar estas problemáticas, orientar en la adopción de buenas prácticas basadas en frameworks, y delinear los aspectos esenciales a considerar según el tipo de empresa u organización.

El panorama global de la ciberseguridad presenta un problema que las organizaciones no pueden ignorar: las amenazas cibernéticas son cada vez más sofisticadas y capaces de causar daños significativos, desde la paralización de operaciones hasta la erosión de la confianza de los personas Esta creciente complejidad hace imprescindible que la ciberseguridad se integre profundamente en la estrategia corporativa, abarcando no sólo los aspectos técnicos, sino también los riesgos financieros y reputacionales.

Sin embargo, dentro de este contexto desafiante también surge una oportunidad. La Política y Estrategia Nacional de Ciberseguridad proporcionará una guía estratégica que ayudará a las organizaciones a fortalecer su resiliencia frente a las amenazas cibernéticas. Establecerá lineamientos estratégicos que incluirán la adopción de buenas prácticas basadas en estándares definidos, la evaluación continua de vulnerabilidades, y la implementación de medidas de prevención y respuesta eficaces. La adopción de estas directrices no sólo mitigará riesgos, sino que también convertirá la ciberseguridad en un elemento clave de competitividad. Al implementar estas estrategias de manera efectiva, las organizaciones no solo protegerán sus operaciones, sino que también mejorarán su reputación y aumentarán la confianza dentro del ecosistema. Esto les permitirá asegurar la continuidad del negocio, incluso en un entorno digital cada vez más incierto.

En resumen, aunque la ciberseguridad plantea serios desafíos, la Política y Estrategia Nacional de Ciberseguridad ofrece la oportunidad de transformar estos desafíos en ventajas estratégicas. Integrar estos lineamientos en la estrategia corporativa permitirá a las organizaciones no solo responder de manera más eficaz a las amenazas actuales, sino también prepararse para los riesgos futuros, asegurando así su capacidad para prosperar en un mundo digital en rápida evolución.

→Factores de la dimensión

Los factores que componen la dimensión son los siguientes:

- Factor 1.1: Estrategia Nacional de ciberseguridad
- Factor 1.2: Respuesta a incidentes y gestión de crisis
- Factor 1.3: Protección de Infraestructura crítica (IC)
- Factor 1.4: Ciberseguridad en defensa y seguridad nacional

→*Stakeholders*

- Organizaciones Gubernamentales
- Organizaciones Privadas
- Fundaciones
- Ciudadanos
- Organizaciones Educativas (Universidades e Institutos)
- Otros interesados

→Objetivos

Objetivo General

Establecer las directrices necesarias para la formalización de la Política y Estrategia Nacional de ciberseguridad en sus cuatro factores, con el fin de gestionar la ciberseguridad nacional y resiliencia frente a eventos, incidentes o hallazgos para sectores públicos- privados y permitiendo cumplir con los nuevos requisitos impuestos en la Ley Marco de Ciberseguridad N°21.663.

Objetivos por factor	
Factor 1.1: Estrategia Nacional de ciberseguridad	Desarrollar una estrategia nacional de ciberseguridad que asegure la protección de la infraestructura crítica (servicios esenciales), con el fin de otorgar seguridad a los datos de los ciudadanos de la nación.
Factor 1.2: Respuesta a incidentes y gestión de crisis	Establecer un proceso integral de respuesta ante incidentes que permita a la nación prevenir y gestionar de manera eficaz una crisis de ciberseguridad.
Factor 1.3: Protección de Infraestructura crítica (IC)	Establecer y gestionar diferentes actividades de protección para garantizar la continuidad, disponibilidad e integridad de las infraestructuras críticas definidas, con el fin de resguardar la continuidad de las operaciones y funciones.
Factor 1.4: Ciberseguridad en defensa y seguridad nacional	Consolidar un plan de defensa de ciberseguridad (público-privado) preventivo, con el fin de resguardar la seguridad a nivel nacional.

→Impacto

El impacto esperado de la Política Nacional de Ciberseguridad es la creación de un entorno digital más seguro, resiliente y confiable, donde los ciudadanos, las empresas y la infraestructura crítica estén protegidos de manera efectiva. Esta política garantizará la continuidad operativa de las organizaciones públicas y privadas, minimizando las interrupciones causadas por ciberataques y creando un ambiente de producción seguro. Además, fomentará la innovación tecnológica con un enfoque soberano, promoviendo el desarrollo de capacidades nacionales que permitan a largo plazo ganar mayores niveles de control sobre las tecnologías críticas, reduciendo la dependencia externa.

Permitirá la creación de planes y estrategias para enfrentar escenarios en donde la complejidad de los incidentes de ciberseguridad ponga en riesgo la seguridad nacional y, por tanto, fortalecerá las herramientas tanto tecnológicas, como de gestión, para dar respuesta a las probables crisis asociadas. Es de vital importancia para la continuidad del funcionamiento del Estado de Chile, contar con la debida coordinación, cooperación e interoperatividad que permitan la protección de la infraestructura crítica, así como también, la contención y mitigación de impactos en escenarios catastróficos.

FACTORES DE LA DIMENSIÓN

→FACTOR 1.1. ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

→Antecedentes generales

La estrategia de ciberseguridad es esencial para la transversalización de una agenda de ciberseguridad en todo el gobierno, dado que contribuye a priorizar la ciberseguridad como un área de política clave, determina responsabilidades y mandatos de actores gubernamentales claves en materia de ciberseguridad, y determina la asignación de recursos para problemas emergentes, existentes y prioridades en ciberseguridad. Fuente: Foro Nacional de Ciberseguridad, Gobierno de Chile.

→Problemáticas

Para comprender y abordar de manera efectiva las problemáticas relacionadas con la Estrategia Nacional de Ciberseguridad, se pueden identificar dos enfoques complementarios:

Enfoque estratégico técnico: Este enfoque se centra en la importancia del control sobre las tecnologías críticas utilizadas en el país. La falta de soberanía tecnológica es una problemática clave, ya que la dependencia de tecnologías extranjeras limita la capacidad del país para gestionar la ciberseguridad de manera autónoma y efectiva.

→Problemas identificados:

• **Dependencia tecnológica externa:** La infraestructura crítica y los sistemas de seguridad digital dependen de tecnologías desarrolladas en el extranjero, lo que aumenta el riesgo de vulnerabilidades no controladas.

• **Falta de desarrollo tecnológico propio:** Hay una baja inversión en investigación y desarrollo de tecnologías locales, lo que dificulta la creación de soluciones adaptadas a las necesidades nacionales.

• **Limitada capacidad de respuesta autónoma:** Ante un incidente cibernético, el país depende de proveedores externos para solucionar problemas o realizar actualizaciones críticas, lo que reduce la autonomía en la gestión de ciber amenazas.

Enfoque Estratégico Normativo: Se plantea la necesidad de contar con un marco normativo sólido y actualizado que establezca las directrices estratégicas en ciberseguridad. Esto incluye la implementación de políticas públicas que faciliten la coordinación efectiva entre los sectores público y privado, el cumplimiento de normativas y el fomento de una cultura de seguridad digital en todos los niveles.

→Problemas identificados:

• **Fragmentación normativa:** Las regulaciones en ciberseguridad no están unificadas ni alineadas con las mejores prácticas internacionales, lo que genera vacíos legales y confusión en su implementación.

• **Escasa coordinación público-privada:** Falta de estructuras formales para compartir información crítica sobre ciber amenazas y coordinar respuestas rápidas y eficaces ante incidentes, con el fin de garantizar la protección de la información sensible o critica de cada empresa o secretos de estado.

• **Falta de capacitación y concienciación:** No existe una cultura de ciberseguridad arraigada en la sociedad y en las organizaciones, lo que genera un bajo nivel de conocimientos y preparación ante amenazas cibernéticas.

• **Inexistencia en identificación de los recursos presupuestarios:** No existe un ítem presupuestario a nivel de gobierno que sea específico, para se pueda identificar y asegurar los recursos a la Ciberseguridad, tal como se realiza para otras designaciones (por ejemplo: servicios informáticos o equipamiento).

→Efectos del problema

• **Pérdida de datos:** La falta de políticas claras sobre la protección de la información puede resultar en la pérdida o encriptación de datos sensibles, afectando tanto a organizaciones públicas y privadas como también a los ciudadanos.

• **Costos financieros elevados:** Los incidentes cibernéticos mal gestionados provocan costos financieros elevados, debido a la inversión necesaria para recuperarse de los ataques, que podrían haberse prevenido o mitigado con políticas adecuadas.

• **Daño reputacional:** Las organizaciones y el Estado pueden sufrir una pérdida de confianza por parte de los ciudadanos y las empresas, lo que puede conllevar sanciones regulatorias y la erosión de la credibilidad.

• **Interrupción operativa:** Las ciber amenazas, como el malware, las brechas de seguridad o los ataques distribuidos de denegación de servicio (DDoS), pueden interrumpir las operaciones de organizaciones clave. Sin una estrategia robusta, estas interrupciones en servicios críticos pueden tener consecuencias severas para la infraestructura del país.

• **Aumento de vulnerabilidades:** La falta de lineamientos estratégicos deja brechas de seguridad sin abordar, lo que incrementa las vulnerabilidades en infraestructuras críticas y sistemas digitales, exponiéndolos a ataques cibernéticos más frecuentes.

• **Dependencia tecnológica externa:** Al no existir un marco estratégico que promueva el desarrollo tecnológico nacional, la dependencia de soluciones extranjeras continúa, perpetuando la falta de control sobre las tecnologías críticas y aumentando los riesgos asociados.

• **Incapacidad para coordinar respuestas a incidentes:** Sin lineamientos claros, la cooperación entre los sectores público y privado es ineficiente, lo que retrasa la respuesta ante incidentes cibernéticos y agrava los daños.

• **Desactualización frente a amenazas emergentes:** Sin un marco estratégico flexible y actualizado, las organizaciones y el Estado no pueden adaptarse rápidamente a nuevas amenazas cibernéticas, exponiéndose a ataques que utilizan tecnologías o métodos novedosos.

Propuesta Ámbito IT

→POLÍTICA DE PROTECCIÓN PARA IT:

Descripción: Establecer una política integral que impulse la implementación de plataformas seguras en todos los sistemas de TI. Esta política debe definir estándares, mejores prácticas y marcos de trabajo, para asegurar que los sistemas de TI se construyan y mantengan con los más altos niveles de seguridad, garantizando la protección desde el diseño. La reducción de la superficie de ataques e implementación de medidas preventivas es clave.

Normativas aplicables:

- **NIST CSF (Protect):** Gestión de acceso, protección de datos, uso de firewalls y segmentación de redes.

- **ISO 27001:** Establece requisitos de seguridad de la información, incluyendo políticas de control de acceso y protección de datos.

- **NIS2:** Asegura que las empresas implementen controles adecuados para la protección de los sistemas de información.

→SEGURIDAD EN EL DISEÑO DE INFRAESTRUCTURAS DE TI:

Descripción: Asegurar que la protección esté integrada desde el diseño de las infraestructuras de TI. Esto incluye definir políticas que requieran una revisión de seguridad en cada etapa del ciclo de vida de desarrollo de sistemas y software.

Normativas aplicables:

- **ISO 27001 (ISO27001), 22237 (ISO22237), 27035 (ISO 27035), 22301 (ISO22301), y NIST CSF:** Protección desde el diseño, revisiones de seguridad, y análisis de vulnerabilidades antes de la implementación de cualquier nuevo sistema.

→MONITORIZACIÓN DE SISTEMAS DE TI:

Descripción: Implementar soluciones avanzadas de monitoreo continuo para detectar amenazas en tiempo real y tomar acciones preventivas antes de que se materialicen. Esto incluye el uso de herramientas SIEM (Security Information and Event Management).

Normativas aplicables:

- **NIST CSF (Detect):** Soluciones de monitoreo continuo y detección de anomalías.

- **ISO 27001:** Requiere procesos de supervisión y revisión continua de sistemas.

• **ISO 22237:** Estándar sobre los requisitos y recomendaciones para la construcción de instalaciones e infraestructura de centro de procesamiento de información.

• **ISO 27035:** Gestión de Incidentes de Seguridad Informática.

• **ISO 22301:** Estándar de aplicabilidad sobre seguridad y Resiliencia, Gestión de la Continuidad del Negocio - Requerimientos

→Propuesta Ámbito OT

POLÍTICA DE PROTECCIÓN PARA OT:

Descripción: Definir una política específica para la protección de plataformas y sistemas OT, garantizando que las infraestructuras operativas (como energía, transporte y manufactura), según el acuerdo NIS2, acordado, cuentan con las medidas adecuadas para proteger los sistemas de control industrial (ICS) , SCADA, Modbus entre otros.

Normativas aplicables:

• **NIST CSF (Protect):** Protección física y lógica de sistemas operativos, segmentación de redes OT y gestión de accesos.

• **NIS2 y NCSC:** Definen directrices claras para infraestructuras críticas y sistemas OT. con c/u de sus protocolos de comunicación

• **Objetivo:** Asegurar que los sistemas operativos críticos estén protegidos de ataques cibernéticos que puedan afectar su funcionamiento.

→SEGMENTACIÓN DE REDES Y CONTROL DE ACCESO EN ÁREAS CRÍTICAS DE OT (SEGMENTADAS Y NO SEGMENTADAS):

Descripción: Implementar una segmentación estricta entre las redes TI y OT, garantizando que los sistemas operativos críticos no se vean comprometidos por amenazas provenientes de las redes IT. Además, establecer controles de acceso robustos y específicos para OT.

Todo dispositivo conectado a industria crítica y/o OT debe incluir accesos básicos basados en RBAG, RSA y MFA, con su consiguiente proceso normativo.

Normativas aplicables:

• **NIST CSF (Protect):** Establecimiento de políticas de segmentación de redes y control de acceso.

• **Modelo bajo norma ISA/IEC 62443:** correlacionado con el modelo purdue desde el ámbito 0 en adelante.

Además de regirse tanto el CSIRT de IC, como todo control, actualización y futuras políticas en las normas y estándares provenientes de ICS4ICS, incluidos temas de transporte tanto marítimos, aéreos como terrestres.

Exigencias normativas:

• Poseer Mapa de Riesgo de infraestructura Crítica completa, con seguimiento mensual y puntos de mejora. Las exigencias normativas incluyen la obligación de contar con un Mapa de Riesgo de Infraestructura Crítica completo, con seguimiento mensual y puntos de mejora identificados, disponer de un plan de contingencia real que sea probado trimestralmente, con evidencia documentada de su implementación y realizar una verificación anual de estos puntos a cargo de la ANCI y el CSirt, según corresponda.

• Poseer contingencia real y plan de pruebas de forma trimestral de la misma, con evidencia de la realización.

• verificación de los puntos anteriores anualmente, por ANCI y CSirt según corresponda.

→MONITORIZACIÓN Y RESPUESTA EN OT

Descripción: Desplegar herramientas de monitorización en tiempo real y respuesta a incidentes en sistemas OT. Esto incluye la integración de soluciones de seguridad cibernética para detectar anomalías en procesos industriales.

Normativas aplicables:

• **NIST CSF (Detect y Respond):** Soluciones de detección de amenazas y respuesta a incidentes en sistemas de control industrial.

• **ISA/IEC 62443:** Define procesos de respuesta ante incidentes y la necesidad de monitorear continuamente los sistemas OT.

→FACTOR 1.2: RESPUESTA A INCIDENTES Y GESTIÓN DE CRISIS

→Antecedentes Generales

La respuesta a incidentes y gestión de crisis es un proceso clave al definir e implementar las estrategias de ciberseguridad en toda organización, ya sea pública o privada. Identificar las principales etapas de este proceso, permite responder de manera clara y estructurada cuando se materializan incidentes de ciberseguridad que impactan en el negocio.

→Problemáticas

Una de las principales problemáticas referidas a la respuesta de incidentes y gestión de crisis, se produce en la falta de preparación y en la aplicabilidad de protocolos por parte de las organizaciones de Chile, si bien contamos a nivel país con un equipo de respuesta de incidentes en ciberseguridad CISRT (https://csirt.gob.cl/), dependiente del ministerio del interior y seguridad pública, no basta con el apoyo en la indagatoria en los acontecimientos que materializaron la contingencia, sino más bien se requiere de un acompañamiento en la evaluación del impacto, con el objeto de apoyar en la restauración de funciones, además de la gestión y control de las crisis que se presentan cuando este nivel de riesgos es materializado.

→Causas de las problemáticas

- **Presencialidad:** Existe una falta de presencialidad física, cuando graves contingencias son presentadas en cada incidente de ciberseguridad, no existe el apoyo "in situ", para una asistencia profesional en la ejecución de la respuesta y el control de crisis que sufren el o los afectados.

- **Capacidad Preventiva:** No existe una aplicabilidad constante de medidas preventivas en materias de ciberseguridad, como procesos de parchado y actualización de hardware, software y equipamiento TO, que permita establecer mecanismos de prevención ante ataques materializados por medio de la explotación de vulnerabilidades conocidas a informadas.

- **Idoneidad:** Falta de capacidades profesionales y gobernanzas internas en las instituciones, para abordar las contingencias por personal idóneo, capacitado y vinculante a este tipo de situaciones.

→Efectos del problema

Tardanza en los tiempos de reacción por parte de las instituciones, existiendo en algunos casos un aumento en la gravedad de la contingencia por falta de orientación experta "in situ".

Desorientación y descoordinación ante la imprevista materialización de contingencias graves, tanto en la asistencia legal como técnica, dado que no se mantienen políticas ni procedimientos formalizados que definan el conjunto de acciones para estos casos. Y finalmente la falta de conocimientos de empresas relacionadas (cadena suministro) que pueden verse afectadas en incidentes, además de proveedores y otras empresas relacionadas.

→Propuestas

→Ámbito IT y OT

Establecer una Política de Respuesta de Incidentes y Gestión de Crisis, teniendo en cuenta paralelamente que, para la gestión de crisis, se debería considerar la generación de un comité de crisis, con la participación obligatoria del equipo CSIRT de gobierno y principalmente la participación del organismo afectado según corresponda, dentro de las

actividades a realizar en vías del transcurso del tiempo, se sugiere lo planteado en la siguiente imagen.

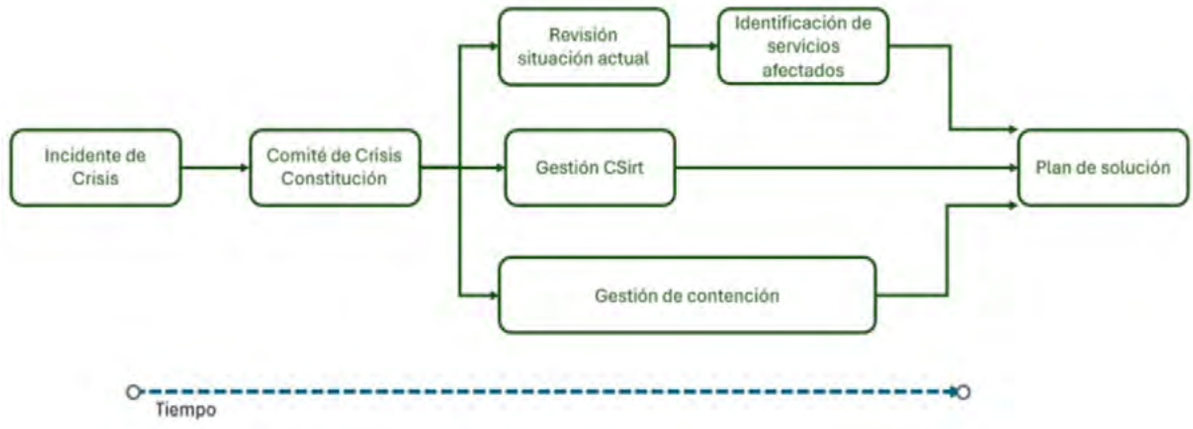


Figura 1: Gobierno de Crisis – Nivel 0

→Política de Respuesta a Incidentes y Gestión de Crisis

Descripción: Corresponde al establecimiento de lineamientos generales y de declaración de intencionalidad por medio de una política que permita establecer alcances, objetivos, procesos y actividades para la gestión de incidentes y gestión de crisis, cabe mencionar que los escenarios contemplados en ésta política son los contemplados en la materialización de riesgos altamente críticos con afectación de servicios masivos, entregados a la ciudadanía, a causa de factores externos, sean estos intencionales y deliberados o accidentales.

Objetivo: Establecer una Política de Gestión de Incidentes y Gestión de Crisis, basada en estándares de uso mundial (ISO 27035), donde se señalen los procesos y actividades generales para la correcta aplicabilidad de las acciones ante un incidente de seguridad de la información y ciberseguridad, además de las coordinaciones y procedimientos que sean idóneos para la gestión de crisis en los sectores y servicios afectados (Deberán existir roles definidos, como por ejemplo: comunicación, líder del evento, etc).

Preparación: La adopción de una Política de Respuesta a Incidentes y Gestión de Crisis, presupone que tanto las organizaciones del Sector Público como el Sector Privado tengan una etapa de preparación en donde ajustar los estándares mínimos que permitirán a las organizaciones afrontar la gestión y respuesta de incidentes. Al respecto es importante señalar, que en cuanto a la gobernanza del proceso a nivel país, es decir, a la gobernanza de la ciberdefensa en términos de infraestructura crítica, esta preparación demandará tener claramente identificadas las organizaciones que deberán participar en las distintas etapas del incidente, así como también, los roles, responsabilidades y recursos involucrados. Por tanto, para efectos de la respuesta a incidentes y gestión de crisis de infraestructura crítica o de una respuesta y gestión a nivel país, es necesario, homólogamente hablando, contar con la definición y catastro de las infraestructuras críticas a proteger, siendo oportuno en esta parte que la Agencia Nacional de Ciberseguridad, establezca qué infraestructura, servicios y organizaciones, contarán con el carácter de Infraestructura Crítica, Servicio Esenciales y Operadores de Importancia Vital, toda vez que, permitirá la oportunidad y aclaración a un mejor enfoque en los modelos de gestión y de negocios a los privados, como también, direccionar los esfuerzos a las autoridades fiscalizadoras para velar por el cumplimiento de requisitos normativos, de manera transversal como sectorial, desde cordillera a mar.

En segundo punto, cuando hablamos de gestión de crisis, necesariamente estamos hablando de un incidente que compromete gravemente algún aspecto de la confidencialidad, integridad y disponibilidad de nuestros activos de información o de la infraestructura crítica, que desde lo técnico podría tener más facilidad para ser analizado y evaluado, que, para los altos directivos o autoridades, sobre todo en el sector público. Para estos efectos, es necesario también preparar a todos los funcionarios públicos que estén en el nivel directivo, y que den el tono a la organización (Tone at the Top según COSO*), para que faciliten las labores de gestión y respuesta comprendiendo a cabalidad los riesgos, amenazas e impactos que están asociados a un incidente de alta complejidad. Adicionalmente, la etapa de preparación debe considerar la identificación de brechas en las capacidades de gestión y respuestas para ser mejoradas en lo inmediato, así como también incluir al menos Planes de Gestión y Respuesta ante Incidentes, Planes de Continuidad Operacional, Planes de Gestión de Crisis y Planes de Recuperación ante Desastres, definidos tanto para cada organización, como para la respuesta a un incidente de alta complejidad generalizado, explicitando Roles, Responsabilidades, Puntos de Contacto, Canales de Coordinación Interinstitucionales, Comunicaciones internas y externas, Monitoreo de amenazas y persistencia, entre otros.

Toda vez que se materialice un incidente se debería considerar:

- Revisión del estado actual
- Identificación de Servicios Afectados
- Gestión de CSIRT
- Consulta de Playbooks
- Comité de Crisis
- Gestión de Contención
- Plan de Remediación
- Lecciones Aprendidas y Mejora Continua

Vinculación a los Comité Operativo de Emergencia - Directivos y Técnicos (COE)

Normativas Aplicables:

- **ISA / IEC 62443 PRINCIPAL**

Secundarias

- **ISO 27001 (ISO27001):** Estándar sobre los requisitos de los Sistemas de Gestión de Seguridad de la Información

- **ISO 27035 (ISO27035):** Estándar sobre la Gestión de Incidentes de Seguridad de la Información

- **Ley Marco de Ciberseguridad N°21663:** establece la obligación de reportar incidentes de ciberseguridad

→FACTOR 1.3 PROTECCIÓN DE INFRAESTRUCTURA CRÍTICA (IC)

→Antecedentes generales

Este factor estudia la capacidad del gobierno para identificar activos de IC, los requisitos regulatorios específicos de ciberseguridad de la IC y la implementación de buenas prácticas en materia de ciberseguridad por parte de los operadores de IC.

- **Identificación:** este aspecto aborda la existencia de una lista general de activos, sectores y operadores de IC, y una auditoría de los activos de IC de forma periódica;

- **Requisitos regulatorios:** este Aspecto aborda la existencia de requisitos regulatorios específicos para la ciberseguridad de la IC

- **Práctica operativa:** este aspecto explora si los operadores IC implementan estándares reconocidos de la industria

→Problemáticas

La protección de la IC es un tema muy importante para la seguridad nacional de nuestro país, cuya interrupción o daño, nos podría dar graves consecuencias para nuestra sociedad, produciendo la paralización de varios servicios críticos del país. Siendo un tema de alta criticidad, en el cual, se debe trabajar fuertemente en la mitigación de esta problemática.

Por otro lado, se debe considerar que varios servicios esenciales de diferentes tipos de industrias, de cordillera a mar, deben ser evaluados y potencialmente categorizados para ser denominados como infraestructura crítica, acordes a la definición establecida en la Ley 21.663 y la Ley 21.542, donde en lo que importa, se plantean los conceptos de Infraestructura Crítica, Servicios Esenciales y los operadores de Importancia vital, lo anterior, basado 100% en el acuerdo NIS2 y toda aquella norma, acuerdos o estándares industriales IT/OT y marcos regulatorios establezcan a nivel nacional, tarea que debe asumir la nueva Agencia Nacional de Ciberseguridad, en los términos que se plantearon en la Política de Respuesta a Incidentes y Gestión de Crisis, difundiendo directrices a las Autoridades Fiscalizadoras sectoriales y transversales, como también reforzando los respectivos requisitos de cumplimiento del marco normativo y frameworks de la industria de interés a las organizaciones público-privadas. Las autoridades fiscalizadoras deberán mantenerse actualizadas en el estado del arte y asumir procesos de capacitaciones y preparación de la gestión del conocimiento acorde a la evolución de la insdustria y su entorno comercial regional e internacional, avalando y reforzando todo el proceso que el desarrollo tecnológico y de IT/OT exige la 4ta rev. Ind.

→Causas de las problemáticas

Algunas de las principales causas de la problemática de la protección de la IC con respecto a la interrupción o daño en sus servicios son los siguientes:

- **Amenazas naturales:** las causas naturales como un terremoto, incendio o inundaciones a un servicio de IC, podría interrumpir o detener por completo el funcionamiento normal de estos servicios críticos.

• **Ciberataques:** los ciberataques han ido creciendo notablemente en la actualidad y seguirán aumentando en el futuro, con nuevas tácticas, las cuales pueden afectar las IC de los distintos servicios críticos, los cuales se deben resguardar su funcionamiento e información que puedan manejar.

• **Interdependencias de sectores:** Cada sector de la IC están interconectados, ya que entre ellas pueden dar servicios a otros, por lo que si un servicio crítico falla, como por ejemplo el servicio de energía, los servicios que requieren de este, pueden desencadenar un problema aún mayor a las IC.

• **Falta de Concientización y Capacitación del Personal Operativo:** La ciberseguridad en la IC requiere que todos los niveles de personal estén capacitados para reconocer y responder ante amenazas. Sin embargo, en muchos casos, el personal que opera los sistemas críticos no cuenta con formación específica en prácticas de ciberseguridad y gestión de incidentes, aumentando la probabilidad de que ocurran errores humanos que comprometan la seguridad y funcionalidad de la IC.

• **Obsolescencia de Equipos y Falta de Actualización de Infraestructuras:** Una gran parte de la infraestructura crítica puede estar operando con equipos y sistemas heredados que no fueron diseñados para soportar ciberataques modernos o para integrarse con tecnologías avanzadas. Esta obsolescencia puede dejar abiertas múltiples vulnerabilidades que los atacantes pueden explotar, poniendo en riesgo la seguridad y operatividad de la IC. La falta de recursos y de programas de actualización adecuados agravan esta problemática, reduciendo la capacidad de defensa de estos sistemas frente a amenazas actuales.

• **Carencia de Normativas y Requisitos Regulatorios Claros:** Aunque existen marcos regulatorios aplicables, en muchos casos no están completamente adaptados a los desafíos actuales de ciberseguridad en las IC. La falta de normativas específicas y actualizadas crean vacíos de protección y dejan a la IC vulnerable a incidentes. Además, la falta de auditorías regulares limita la capacidad de los operadores para identificar y mitigar vulnerabilidades.

• **Presupuesto Limitado y Escasez de Recursos:** La protección de la IC requiere una inversión constante en tecnología, capacitación de personal y mantenimiento de los sistemas. Sin embargo, los recursos asignados frecuentemente no son suficientes para cubrir estas necesidades, lo que genera una brecha en la seguridad. La falta de presupuesto induce a priorizar otros aspectos operacionales, dejando en segundo plano las inversiones en seguridad y actualizaciones críticas.

• **Limitación en la Colaboración entre Sectores Público y Privado:** La IC está compuesta tanto por instituciones gubernamentales como privadas, lo que hace necesario un enfoque colaborativo para su protección. La falta de cooperación e intercambio de información entre los sectores público y privado dificulta la implementación de un enfoque integral de seguridad.

→Efectos del problema

→INTERRUPCIÓN DE SERVICIOS:

• **Infraestructura Crítica:** La interrupción de servicios esenciales, como el suministro de energía, telecomunicaciones, y servicios bancarios, puede ser crítica. Estos sectores son fundamentales para el funcionamiento diario del país, y su afectación podría llevar a una disrupción generalizada en la economía y en la vida cotidiana de la población.

• **Servicios Públicos y Privados:** Si una amenaza compromete la ciberseguridad de servicios del gobierno o de entidades privadas, puede generar parálisis en áreas como salud, educación y transporte, dificultando el acceso de los ciudadanos a servicios básicos.

→IMPACTO EN EL BIENESTAR DE LA POBLACIÓN:

• **Afectación Psicológica:** La interrupción de servicios esenciales puede provocar angustia y ansiedad en la población, especialmente si se ven afectados servicios de emergencia o de salud.

• **Pérdida de Confianza:** Si los ciudadanos perciben que sus datos personales no están protegidos, puede disminuir su confianza en los servicios digitales. Esto puede llevar a una menor adopción de tecnología y a la resistencia en el uso de servicios en línea, afectando la modernización y eficiencia de los servicios públicos y privados.

• **Impacto Económico Personal:** La paralización de servicios financieros, como los bancos, puede hacer que las personas no puedan acceder a su dinero, realizar pagos o recibir sus salarios a tiempo, afectando directamente su economía personal.

• **Vulnerabilidad en la Salud:** La ciberseguridad en el sector salud es crítica. Si una amenaza impide el acceso a los registros médicos o interfiere con los sistemas de emergencia, podría poner en riesgo la vida de los pacientes y complicar el acceso a atención médica en momentos de urgencia.

→Propuestas

Ámbito IT

→POLÍTICA DE PROTECCIÓN PARA IT

Descripción: Implementar una política integral que garantice la protección de los sistemas de TI en todas las infraestructuras críticas. Esta política debe establecer estándares y prácticas de seguridad que aseguren la identificación y protección de los activos de IC.

Objetivo: Reducir los riesgos de interrupción y daño en plataformas TI dentro de la IC mediante autenticación multifactor, cifrado de datos, y procedimientos de respaldo y actualización de sistemas.

Normativas aplicables

- **NIST CSF (Protect):** Gestión de acceso, protección de datos, uso de firewalls y segmentación de redes en entornos críticos.
- **ISO 27001:** Define requisitos de seguridad de la información, incluyendo políticas de control de acceso y protección de datos.
- **NIS2:** Establece controles de seguridad específicos para la protección de infraestructuras críticas.

→SEGURIDAD EN EL DISEÑO DE INFRAESTRUCTURAS DE TI

Descripción: Asegurar la integración de medidas de protección en todas las etapas de diseño de infraestructura de TI para la IC. Esto incluye auditorías de seguridad periódicas y análisis de vulnerabilidades de los sistemas críticos.

Normativas aplicables:

- **ISO 27001, ISO 22237, ISO 22301 y NIST CSF:** Incorporación de la seguridad desde el diseño, evaluaciones de seguridad, y análisis de vulnerabilidades previos a la implementación de sistemas.

Objetivo: Prevenir vulnerabilidades en sistemas TI desde el diseño, reduciendo así el riesgo de fallos en infraestructuras críticas.

→MONITORIZACIÓN DE SISTEMAS DE TI

Descripción: Implementar sistemas de monitoreo continuo, como SIEM, para detectar y responder a amenazas en tiempo real dentro de los sistemas de IC. Esto permite identificar anomalías y prevenir ciberataques que podrían interrumpir los servicios críticos.

Objetivo: Minimizar el tiempo de respuesta ante amenazas, asegurando la disponibilidad de los servicios críticos.

Normativas aplicables:

• **NIST CSF (Detect):** Requiere soluciones de monitoreo continuo para la detección de amenazas.

• **ISO 27001:** Supervisión y revisión continua de sistemas críticos.

• **ISO 27.002:** Buenas prácticas en seguridad de la información, esencial para proteger la integridad y disponibilidad de los sistemas IT/OT, definir medidas de seguridad específicas para los dispositivos y gestionar los riesgos que se derivan de la conectividad entre las dos dimensiones con el objeto de mitigar las vulnerabilidades al gestionar la protección de activos de la información de carácter sensible.

• **ISO 27.005:** Gestión de riesgos de seguridad de la información, relevante en los procesos de levantamiento al identificar, evaluar y acortar brechas en los riesgos específicos de los sistemas del modelo de negocio, priorizando equipos críticos, evaluar el potencial impacto de los riesgos en ellos y gestionar la implantación de planes de respuesta y mitigación específicos para mantener la protección y continuidad del negocio de las operaciones industriales de la infraestructura crítica.

• **ISO 22301:** Continuidad del negocio y resiliencia.

Ámbito OT

→POLÍTICA DE PROTECCIÓN PARA INFRAESTRUCTURAS DE OT

Descripción: Crear una política específica de seguridad para redes y sistemas OT, aplicable a todos los sectores de IC, que considere la segmentación y separación de redes OT y TI para proteger los activos críticos.

Objetivo: Proteger las redes OT en infraestructuras críticas de posibles accesos no autorizados y evitar que ciberataques afecten el funcionamiento de los servicios esenciales. se debe a su vez cruzar 1 vez por año la normativa de control y ciberseguridad con SANS y/o ISACA.

Normativas aplicables

• **NIST SP 800-82:** Establece controles de ciberseguridad en sistemas industriales, entregando recomendaciones para la seguridad de los sistemas de control industrial (ICS), tales como gestión de configuraciones, monitoreo de eventos y estrategias de respuesta ante poetenciales incidentes.

• **IEC 62443:** Normativa de seguridad para sistemas de control y automatización en ambientes industriales, centrado en la ciberseguridad ICS y estableciendo requisitos para los fabricantes, operadores e integradores de sistemas OT, definiendo prácticas para la segmentación de redes, controles de acceso, gestión de riesgos y respuesta ante incidentes, complementando ambientes aislados y protegidos OT.

• **NIS2:** Establece requisitos de ciberseguridad para operadores de Servicios Esenciales e Infraestructuras críticas, exigiendo medidas de seguridad efectivas y la responsabilidad en la notificación de cualquier potencial incidente que impacte en la continuidad del negocio.

• **Ley 21.719 (Protección de la vida privada - GDPR):** Ante las potenciales implicancias para las dimensiones tanto OT como IT, cuyas infraestructuras recopilan o procesan datos para cada dimensión en la habilitación y acceso a los ambientes respectivos, al momento de integrar los datos personales de los colaboradores, clientes o usuarios en controles de acceso, acceso a los sistemas y al momento de emplear las plataformas respectivas al interior de las organizaciones y su interacción con sus Stakeholders.

→MANTENIMIENTO Y ACTUALIZACIÓN DE EQUIPOS OT

Descripción: Realizar mantenimiento y actualización continua de firmware y software en equipos OT en sectores críticos, reduciendo así el riesgo de fallos y vulnerabilidades en infraestructuras vitales.

Objetivo: Evitar vulnerabilidades en equipos OT mediante un mantenimiento periódico que asegure su resiliencia y operación.

Normativas aplicables:

• **NERC-CIP**

• **IEC 62443-2-1:** Seguridad en el ciclo de vida de sistemas de control industrial.

• **ISO 27001:** Mantención de la seguridad en infraestructuras críticas.

→SEGURIDAD FÍSICA EN INFRAESTRUCTURA OT

Descripción: Implementar controles de acceso físico y medidas de seguridad en ubicaciones críticas donde se encuentren equipos OT, protegiéndolos contra accesos no autorizados y manipulaciones físicas.

Objetivo: Asegurar la protección física de los equipos OT en sectores críticos, limitando el acceso solo a personal autorizado.

Normativas aplicables

- **NIST SP 800-82:** Controles de seguridad física para sistemas industriales.
- **ISO 22301:** Continuidad del negocio y protección de infraestructuras críticas.

→PLAN DE RESPUESTA A EMERGENCIAS Y RECUPERACIÓN EN OT

Descripción: Desarrollar un plan específico de recuperación ante desastres y de respuesta a incidentes para infraestructuras OT. Este plan debe incluir protocolos para la restauración rápida de servicios en caso de desastres naturales o ciberataques.

Objetivo: Garantizar la continuidad de los servicios críticos y reducir al mínimo el tiempo de inactividad de las infraestructuras en situaciones de emergencia. la Ley N° 21.542, publicada el 3 de febrero de 2023, permite que las Fuerzas Armadas protejan la infraestructura crítica del país en caso de peligro grave o inminente.

Normativas aplicables:

- **ISO 22301:** Continuidad del negocio y resiliencia.
- **NIST CSF (Respond):** Directrices para la recuperación de incidentes de seguridad.

→FACTOR 1.4 CIBERSEGURIDAD EN DEFENSA Y SEGURIDAD NACIONAL

Antecedentes Generales

La Ley N° 21.542 en Chile, también conocida como la Ley de Infraestructuras Críticas de la Información (ICI), representa un marco regulatorio esencial para la protección de infraestructuras críticas, incluidas aquellas que operan en entornos de tecnología operativa (OT) industrial. Aprobada en agosto de 2023, esta ley tiene como objetivo garantizar la seguridad y resiliencia de las infraestructuras críticas de la información, estableciendo responsabilidades, estándares y procedimientos que permiten mitigar riesgos de ciberseguridad en sectores clave, como control de procesos, automatización y monitoreo en tiempo real, lo que hace indispensable asegurar su integridad, disponibilidad y confidencialidad ante ciber amenazas.

Asimismo, la ley establece la creación de la Agencia Nacional de Ciberseguridad (ANCI), que será el organismo encargado de supervisar la seguridad de las infraestructuras críticas de información en el país. En el contexto OT industrial, la ANCI desempeñará un papel clave en:

- **Supervisar y coordinar medidas de seguridad** que garanticen la protección de los sistemas de control industrial (ICS) y otros entornos OT.

• **Establecer estándares de seguridad mínimos** específicos para la protección de OT y apoyar la resiliencia de estos sistemas.

• **Ofrecer pautas de respuesta ante incidentes y crisis**, lo cual es fundamental en entornos industriales para limitar los impactos de posibles ciberataques o interrupciones.

Por otro lado, las organizaciones que operan infraestructuras críticas de información **adopten medidas de seguridad y controles específicos.** En el ámbito OT, esto significa que:

• **Los sistemas de control industrial (ICS) deben estar protegidos contra amenazas tanto físicas como cibernéticas**, con protocolos específicos adaptados a los entornos OT.

• **Se establecen requisitos de segmentación y protección de redes,** para minimizar el riesgo de que ataques a sistemas IT puedan propagarse a los sistemas OT.

• **Se definen normas de auditoría y monitoreo continuo** de los sistemas OT, lo cual ayuda a detectar anomalías y prevenir incidentes antes de que afecten la operatividad de los procesos industriales.

De igual forma, infraestructuras críticas deben realizar **análisis periódicos de vulnerabilidades y evaluaciones de riesgos.** En el ámbito OT industrial, esta gestión de riesgos es crucial para:

• **Identificar vulnerabilidades específicas de dispositivos y sistemas de control industrial,** muchos de los cuales no fueron diseñados con ciberseguridad en mente y pueden ser vulnerables a ataques.

• **Evaluar el impacto de posibles amenazas sobre la operatividad de las infraestructuras OT,** permitiendo priorizar medidas de protección para los sistemas que son más críticos para el negocio.

• **Implementar planes de mitigación y contingencia,** de manera que se reduzcan los riesgos de interrupciones operativas en caso de ciberataques o incidentes de seguridad.

Finalmente, en esta parte, la Ley N° 21.542 busca crear un entorno de **colaboración y cooperación entre el sector público y privado** para la protección de infraestructuras críticas, implicando que:

• Las empresas industriales con sistemas OT deben **colaborar con la ANCI y otras entidades** en el intercambio de información sobre amenazas, vulnerabilidades y buenas prácticas.

• La **capacitación y sensibilización en ciberseguridad se vuelve obligatoria** para operadores y técnicos de sistemas OT, asegurando que comprendan los riesgos y las mejores prácticas en seguridad.

• La **gestión de ciberseguridad en sistemas OT pasa a ser una responsabilidad compartida,** donde los operadores industriales, junto con la ANCI, buscan aumentar la resiliencia y responder de forma eficaz ante cualquier eventualidad.

→Problemáticas

A continuación se detallan las principales causas, problemáticas, desafíos y efectos diagnosticado en materia de ciberseguridad para el sector de la defensa y la seguridad nacional, siendo oportuno destacar que las tareas del Foro en esta dimensión, no excluye futuras iniciativas y actualización de nuevas normas, políticas o similares que emanen desde la legislación, ratificación de Estado, definición de nuevos marcos regulatorios, estudios o desarrollo de nuevas tecnologías, siendo oportuno el seguimiento y la mejora continua en los procesos a mediano y largo plazo, como se pretende destacar de manera general en este apartado.

I. Causas de las Amenazas y Vulnerabilidades en Ciberseguridad

• **Aumento de la dependencia digital:** La transformación digital, la adopción de sistemas de tecnología operativa (OT) y la conectividad en infraestructuras críticas aumentan la superficie de ataque, generando más puntos vulnerables, sumado a la condición de clientes "cautivos" con proveedores internacionales de servicios que, en algunos casos ya han presentado vulnerabilidades explotadas por actores maliciosos y potencialmente pueden comprometer la arquitectura y plataformas de la defensa, vulnerando a la seguridad nacional.

• **Proliferación de ciberamenazas globales:** La cibercriminalidad, el espionaje y los ataques por parte de actores estatales y no estatales (potenciales adversarios) están en aumento. Esto incluye amenazas avanzadas persistentes (APTs), ataques de ransomware, y ataques dirigidos a infraestructura crítica e impactando por otro lado, a las instituciones de la defensa.

• **Complejidad de sistemas en defensa y OT:** La interconexión de sistemas de IT y OT, especialmente en entornos de defensa y seguridad nacional, hace que sea más difícil implementar controles de seguridad efectivos, dado que estos entornos suelen incluir tecnologías antiguas y nuevos dispositivos sin medidas de seguridad integradas, sistemas heredados, ausencia de actualizaciones de seguridad y, segmentación externalizada de los servicios de la red de internet.

• **Escasez de masa crítica y especialistas en ciberseguridad:** La falta de profesionales capacitados en ciberseguridad a nivel nacional dificulta el fortalecimiento de defensas adecuadas en sistemas críticos de defensa y seguridad nacional, la gestión del conocimiento y la capacidad de retención del talento, objeto evitar la dispersión del know-how, filtración de información u otro tipo de potenciales vulnerabilidades que puedan ser explotadas desde el factor humano.

II. Principales problemáticas detectadas

• **Fragmentación normativa y regulatoria:** Aunque Chile ha avanzado en la creación de normativas como la Ley de Infraestructura Crítica de la Información, todavía existe una fragmentación en el marco regulatorio, lo cual afecta la coordinación en seguridad nacional. Los sectores de defensa y seguridad nacional requieren regulaciones integradas y adaptadas a las amenazas actuales, debiendo ser sectoriales y transversales que manejen un lenguaje común y sean liderados por la Agencia Nacional de Ciberseguridad.

• **Falta de interoperabilidad entre sistemas de IT y OT:** En entornos de defensa, la falta de interoperabilidad y compatibilidad entre sistemas IT y OT, junto con estándares de ciberseguridad, dificulta la implementación de controles unificados y de estrategias coherentes de protección.

• **Escasa concienciación en ciberseguridad:** En algunos sectores, como el industrial y el de defensa, la concienciación y capacitación en ciberseguridad es limitada. Esto puede derivar en malas prácticas que faciliten el acceso no autorizado a sistemas críticos.

• **Amenazas cibernéticas internacionales:** La defensa y seguridad nacional en Chile están expuestas a amenazas globales, como el espionaje y el sabotaje cibernético, especialmente debido a la creciente actividad de actores estatales y grupos organizados que buscan vulnerar la infraestructura crítica de los países.

III. Desafíos en el Sector de Defensa y Seguridad Nacional

• **Armonización de normas y marcos de ciberseguridad:** La implementación de un marco de ciberseguridad armonizado es crucial para coordinar a las diferentes entidades responsables de la defensa y seguridad nacional (ANCI). Este marco debe incluir normas de seguridad para proteger los sistemas IT y OT y estandarizar la respuesta a incidentes.

• **Desarrollo de capacidades de ciberinteligencia:** Para anticipar, detectar y responder a amenazas avanzadas, Chile debe desarrollar capacidades de ciberinteligencia de potenciales amenazas (internas y externas). Esto incluye infraestructura para el monitoreo y detección de amenazas en tiempo real, especialmente en sectores de infraestructura crítica, servicios esenciales y operadores de importancia vital para el funcionamiento del país.

• **Implementación de estrategias de ciberdefensa:** Un desafío clave es la construcción de una ciberdefensa sólida que incluya no solo la protección pasiva de sistemas, sino también la capacidad de realizar ciberoperaciones para la defensa activa y disuasión ante actores maliciosos, sin tener que depender de proveedores externos que potencialmente puedan coartar la resiliencia operacional, impactando en las capacidades estratégicas de las Instituciones de la Defensa.

• **Fortalecimiento de la colaboración público-privada:** La defensa y seguridad nacional dependen en gran medida de la colaboración con el sector privado, particularmente en el resguardo de infraestructuras críticas que son operadas por empresas privadas (energía, transporte, telecomunicaciones, salud, entre otras relevantes). La cooperación eficaz y el intercambio de información sobre amenazas son esenciales.

IV. Efectos Proyectados de la Ciberseguridad

La implementación efectiva de una estrategia nacional de ciberseguridad en el ámbito de la defensa y seguridad nacional tiene potencialidades y grados positivos al proyectar nuevos desafíos significativos para el desarrollo económico, industrial, social y regulatorio en nuestro país, mediante iniciativas tales como:

• **Protección del desarrollo económico e industrial:** Las infraestructuras críticas y las industrias estratégicas dependen de sistemas seguros. La ciberseguridad contribuye a mantener la estabilidad económica, protegiendo sectores como energía, minería, transporte y telecomunicaciones, que son los motores de nuestra economía.

• **Aumento de la resiliencia en infraestructuras críticas:** Con una estrategia de ciberseguridad adecuada, la infraestructura crítica de los sectores industriales, servicios esenciales y operadores de importancia vital, pueden operar de manera confiable, mitigando el riesgo de interrupciones causadas por ataques cibernéticos.

• **Fortalecimiento de la seguridad nacional:** Al elevar los estándares de ciberseguridad, nuestro país aumenta su capacidad para resistir, gestionar y responder ante potenciales ciberataques que pueden tener efectos perjudiciales para la soberanía, la economía y la estabilidad nacional.

• **Cumplimiento de las normativas internacionales y atracción de inversiones:** A medida que Chile (como política de Estado) se alinease con estándares y buenas prácticas internacionales de ciberseguridad (cuyo mayor o menor grado ya se realiza en las organizaciones, en general), las inversiones extranjeras encontrarán en un entorno más seguro y atractivo para la inversión, lo que beneficiaría el potencial desarrollo y crecimiento económico.

• **Promoción de la gestión del conocimiento y aumento del desarrollo de competencias en ciberseguridad:** Al reconocer y gestionar la necesidad de expertos en ciberseguridad, nuestro país podría desarrollar programas de capacitación y educación de forma continua, fortaleciendo el capital humano y la resiliencia del país en el ámbito digital.

V. Amenazas Potenciales y su Impacto en la Seguridad Nacional

• **Ciberataques disruptivos:** Las infraestructuras críticas, servicios esenciales y los operadores de importancia vital, son objetivos para ataques que pueden paralizar la economía y afectar directamente las actividades de los ciudadanos, economía y potencialmente la seguridad nacional.

• **Espionaje cibernético:** La inteligencia y los datos sensibles de las Fuerzas Armadas y de otras instituciones de la defensa y orden público, son objetivos de espionaje. La amenaza directa a esta información sensible puede comprometer la seguridad nacional.

• **Desinformación y manipulación de la opinión pública:** En un contexto de creciente digitalización, la desinformación puede ser utilizada para debilitar la confianza pública y generar inestabilidad social. La gestión de la ciberseguridad debe incluir medidas para contrarrestar esta amenaza en el ámbito y dimensiones que puedan impactar en la seguridad nacional.

• **Sabotaje industrial y daños económicos:** Los ciberataques son actividades desestabilizadoras, dirigidos a industrias estratégicas, críticas, esenciales y de importancia vital, pueden paralizar la producción, afectar la competitividad y generar pérdidas económicas significativas, cuyos activos no se encuentran considerados en los Ebitda de las organizaciones, lo que subraya la necesidad de proteger entornos OT y sistemas industriales.

→Propuestas

Para ofrecer propuestas tangibles que permitan a Chile reducir la brecha en ciberseguridad en el ámbito de defensa y seguridad nacional, es fundamental diseñar un enfoque estratégico con objetivos a mediano y largo plazo. A continuación, se presentan propuestas para lograr estos objetivos.

I. Establecimiento de un Marco Normativo Integrado

• **Mediano Plazo:** Revisar, actualizar y armonizar las leyes y regulaciones existentes en ciberseguridad para que incluyan requisitos específicos para los sectores de defensa y seguridad nacional. Unificar las normativas que lideren procesos tanto en los sistemas de tecnología de la información (IT) como los de tecnología operativa (OT), invitando a las organizaciones a unirse en el proceso y aunar esfuerzos en el objetivo del desarrollo y protección de los activos en el país.

• **Largo Plazo:** Implementar un marco normativo nacional sólido que abarque ciberseguridad y ciberdefensa, alineado con estándares internacionales y que establezca medidas específicas para la protección de infraestructuras críticas.

II. Desarrollo de Capacidades en Ciberinteligencia y Ciberdefensa

• **Mediano Plazo:** Crear centros de ciberinteligencia especializados en la detección y análisis de amenazas cibernéticas a infraestructuras críticas y en el ámbito de defensa, equipados con tecnología avanzada y recurso humano capacitado.

• **Largo Plazo:** Desarrollar una infraestructura de ciberdefensa autónoma con capacidad de respuesta activa y medidas disuasorias, integrando a expertos en ciberseguridad y ciberinteligencia en los organismos de defensa para una vigilancia continua y coordinada.

III. Fortalecimiento de la Colaboración Público-Privada

• **Mediano Plazo:** Establecer acuerdos de colaboración transversales entre el gobierno, las Fuerzas Armadas y el sector privado que operan infraestructuras críticas, permitiendo un intercambio de información sobre amenazas y mejores prácticas, generando alianzas estratégicas.

• **Largo Plazo:** Contar con el liderazgo directo de la Agencia Nacional de Ciberseguridad, con el objeto de que actúe como un puente entre el sector público y el privado, y que esté encargado de coordinar políticas de seguridad y responder ante emergencias cibernéticas, acortando las brechas a nivel interior y proyectando seguridad y confianza ante la ciudadanía y la industria.

IV. Inversión en Investigación y Desarrollo (I+D)

• **Mediano Plazo:** Financiar proyectos de investigación en ciberseguridad que exploren nuevas tecnologías y metodologías para la protección de infraestructuras críticas y sistemas de defensa.

• **Largo Plazo:** Fomentar la creación y sostenimiento de un ecosistema de innovación en ciberseguridad, estableciendo alianzas con la academia, empresas tecnológicas y centros de investigación que puedan contribuir al desarrollo de soluciones avanzadas en ciberseguridad.

V. Desarrollo de Capital Humano en Ciberseguridad

• **Mediano Plazo:** Iniciar programas de formación especializados para capacitar a profesionales en ciberseguridad con enfoque en defensa y sistemas críticos, apoyando a las universidades y centros técnicos en la creación de mallas curriculares definidas y específicas.

• **Largo Plazo:** Crear un programa nacional de certificación en ciberseguridad para personal en el ámbito de defensa y seguridad nacional, impulsando un sistema educativo de primer nivel en esta materia, con la oportunidad de generar la retención del talento.

VI. Mejoras en la Resiliencia y la Gestión de Incidentes

• **Mediano Plazo:** Establecer políticas claras de gestión de incidentes cibernéticos en sistemas críticos, implementando simulacros y ejercicios de respuesta a ciberataques en sectores clave como defensa, energía, transporte, salud y telecomunicaciones.

• **Largo Plazo:** Fomentar el desarrollo e inversión en una infraestructura de respuesta rápida que permita la continuidad operativa en caso de ciberataques de gran escala, garantizando que los sectores críticos puedan continuar operando durante emergencias cibernéticas.

VII. Concienciación y Cultura de Ciberseguridad

• **Mediano Plazo:** Crear como política país, campañas nacionales de concienciación en ciberseguridad enfocadas en la importancia de la protección de sistemas críticos y el rol de cada persona en el ámbito de seguridad nacional.

• **Largo Plazo:** Integrar ciberseguridad en la cultura de defensa del país, formando a los ciudadanos y a los responsables de la seguridad nacional para que comprendan los riesgos cibernéticos y participen en una defensa colectiva del entorno digital.

VIII. Seguimiento, Análisis, Monitoreo y Evaluación Continua

• **Mediano Plazo:** Implementar un sistema de monitoreo de amenazas que permita la evaluación continua de las políticas y prácticas de ciberseguridad en el país.

• **Largo Plazo:** Establecer una entidad de supervisión permanente que revise y actualice regularmente la estrategia nacional de ciberseguridad, adaptándose a la evolución de las amenazas y los avances tecnológicos, trascendiendo las administraciones de turno.

→Análisis de Viabilidad

La vialidad en este aspecto es sobre las leyes, regulaciones y otros cumplimientos asociados que deberán ser lineamientos por seguir en las organizaciones público-privadas.

Vista Legal	Descripción	Cumplimiento estratégico
Ley Marco de Ciberseguridad 21.663	Obligatorio para las organizaciones públicas y privadas implementen y mantengan medidas de ciberseguridad para la protección de sus datos, sistemas, infraestructura y redes de forma óptima. Exige además la obligatoriedad de dar aviso frente a una manifestación de escenario de vulnerabilidad a la Agencia ANCI.	El establecimiento de Gobierno y la utilización de herramientas además de una definición de estrategia, permite cumplir con los estándares de seguridad establecidos.
Ley de Protección de Datos Personales 21.719	Se requiere asegurar que todo dato personal que sea manejado, almacenado o utilizado por las organizaciones, sea tratado conforme a la ley de protección de datos personales.	Políticas de privacidad y seguridad de los datos personales, en sistemas corporativos y en administración.
Propiedad Intelectual	Gestión de licenciamiento para SW de ofimática y de gestiones relacionadas.	Revisar y dar cumplimiento con las normas de uso de las licencias.
Regulaciones de la Industria	Dar cumplimiento con las normativas específicas de cada sector sector, tales como FINTECH, Salud, Educación, entre otros.	Realizar auditorías y fiscalizaciones internas con el objetivo de asegurar el cumplimiento regulatorio.
Contratos y Acuerdos	Gestionar acuerdos y contratos con colaboradores y/o proveedores con cláusulas de confidencialidad y de manejo de datos personales.	Diseñar y revisar contratos que permitan establecer de forma clara las obligaciones y derechos de cada una de las partes.

Por lo tanto, es importante y viable la generación y aplicabilidad de las propuestas realizadas y en apoyo de la viabilidad analizada.

→DESARROLLO

→Indicadores

Según lo que indica el Documento de niveles de madurez del Foro Nacional de Ciberseguridad, los indicadores *"representan la parte más básica de la estructura de CMM. Cada indicador describe los pasos, acciones o componentes básicos que son indicativos de una etapa específica de madurez. Para haber alcanzado con éxito una etapa de madurez, un país necesita evidenciar cada uno de los indicadores y para elevar la madurez de la capacidad de ciberseguridad de un país, se deberán haber cumplido todos los indicadores dentro de una etapa en particular"*.

En este contexto los indicadores deberán estar alineados con cada uno de los factores de la dimensión y deberán reflejar tanto el diagnóstico actual como el avance, de manera de visualizar claramente el esfuerzo y atención que cada aspecto requiere.

Figura 2: Niveles de Madures Dimensión 1 – Reporte Ciberseguridad 2020 Riesgos, Avances y el Camino a seguir en América Latina y El Caribe

→Instrumento de medición CMM

El CMM es un marco metódico diseñado por el Centro de Capacidades de Ciberseguridad Global (GCSCC, por sus siglas en inglés) de la Universidad de Oxford para evaluar la capacidad de ciberseguridad de un país como mecanismo para lograr una mejor comprensión del estado de su capacidad actual en materia de ciberseguridad y que sea de utilidad en el diseño de las políticas e iniciativas que contribuyan a incrementar su nivel de ciber-resiliencia. La evaluación permite conocer en que etapa de madurez de ciberseguridad se encuentra un país en una escala del 1 al 5; 1 significando etapa inicial y 5 representando una etapa avanzada.

La estructura del modelo del CMM esta divido en las siguientes cuatro (4) secciones: dimensión, factor, aspecto e indicador. Para cada factor y aspecto el CMM propone 5 niveles de madurez, los cuales deberán ser utilizados para medir y hacer seguimiento del avance.

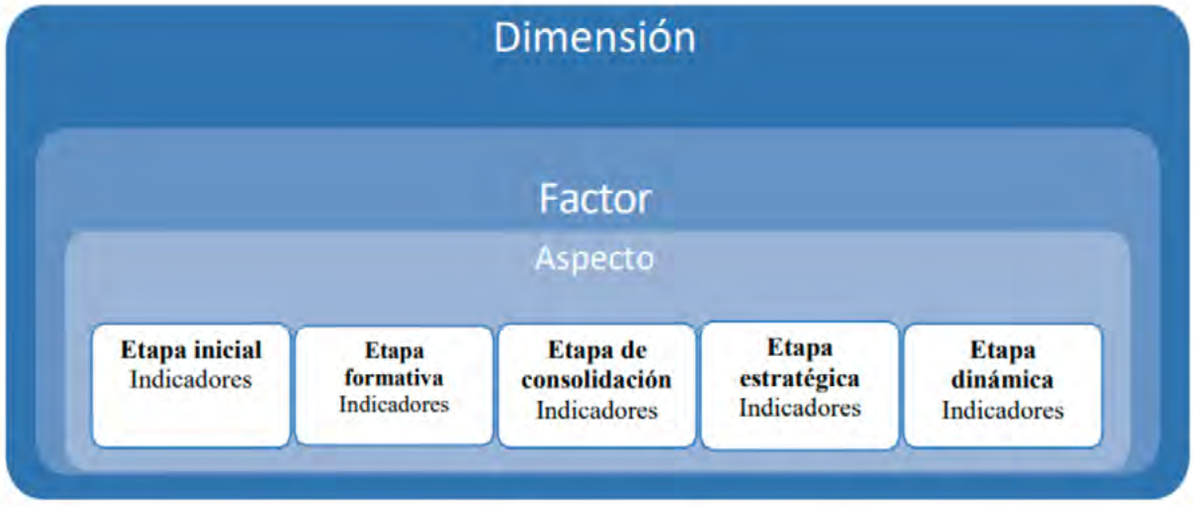


Figura 3: Las 5 etapas de la CMM

Estrategia y Política de Ciberseguridad	Inicial	Formativa	Establecida	Estratégica	Dinámica
Factor 1.1: Estrategia Nacional de ciberseguridad					
Desarrollo de la estrategia					
Contenido					
Implementación y revisión					
Compromiso internacional					
Factor 1.2: Respuesta a incidentes y gestión de crisis					
Identificación y clasificación de incidentes					
Organización					
Integración de ciberseguridad en gestión nacional de crisis					
Factor 1.3: Protección de Infraestructura crítica (IC)					
Identificación de IC					
Requerimientos regulatorios					
Práctica operacional					
Factor 1.4: Ciberseguridad en defensa y seguridad nacional					
Estrategia de ciberdefensa					
Capacidad de ciberdefensa					
Coordinación civil en defensa					

• **Inicio:** En esta etapa, no existe madurez en ciberseguridad o esta es muy embrionaria. Puede haber discusiones iniciales sobre la construcción de capacidades en ciberseguridad, pero no se han tomado acciones concretas. Es posible que no haya evidencia observable en esta etapa.

• **Formativa:** Algunos aspectos han comenzado a desarrollarse y formularse, pero pueden ser ad hoc, desorganizados, poco definidos o simplemente nuevos. Sin embargo, se puede demostrar claramente la evidencia de estas actividades.

• **Establecida:** Los indicadores del aspecto están en su lugar, y la evidencia muestra que están funcionando. Sin embargo, no existe una consideración bien pensada sobre la asignación relativa de recursos. Se han tomado pocas decisiones de compensación relacionadas con la inversión en los diferentes elementos del aspecto. Aun así, el aspecto es funcional y está definido.

• **Estratégica:** Se han tomado decisiones sobre qué partes del aspecto son importantes y cuáles son menos relevantes para la organización o nación en particular. La etapa estratégica refleja que estas decisiones se han hecho considerando las circunstancias específicas de la nación u organización.

• **Dinámica:** En esta etapa, existen mecanismos claros para ajustar la estrategia nacional según las circunstancias prevalecientes, como la tecnología del entorno de amenazas, conflictos globales o cambios significativos en áreas específicas (por ejemplo, ciberdelito o privacidad). También hay evidencia de liderazgo global en temas de ciberseguridad. Al menos los sectores clave han desarrollado métodos para ajustar estrategias en cualquier etapa de su desarrollo. La toma de decisiones rápida, la reasignación de recursos y la atención constante al entorno cambiante son características de esta etapa.

→Conclusiones

De acuerdo con nuestro documento se resalta la urgencia de construir una política robusta de ciberseguridad en Chile, orientada a la protección de infraestructuras críticas, derechos digitales y resiliencia frente a amenazas cibernéticas crecientes. Se destacan los esfuerzos coordinados entre el sector público, privado, la academia y la sociedad civil para avanzar en iniciativas concretas que aborden las problemáticas identificadas.

I. Avances legales y estratégicos

• La promulgación de normativas como la **Ley Marco de Ciberseguridad N°21.663** y la creación de la **Agencia Nacional de Ciberseguridad (ANCI)** son avances significativos.

• Estas normativas permiten proteger infraestructuras críticas y promover la colaboración entre sectores.

II. Principios rectores de la política

• Resiliencia, protección integral, innovación tecnológica, y soberanía digital son pilares fundamentales.

• Se enfatiza la necesidad de estrategias preventivas, basadas en estándares internacionales como ISO 27001, NIST CSF y IEC 62443.

III. Retos y brechas identificadas

• **Falta de soberanía tecnológica:** La dependencia de tecnologías extranjeras y la obsolescencia de sistemas críticos generan vulnerabilidades.

• **Capacitación insuficiente:** Existe una necesidad urgente de formar talento especializado en ciberseguridad.

• **Fragmentación normativa:** La falta de integración de marcos legales dificulta respuestas eficientes a incidentes.

IV. Propuestas estratégicas

• Establecimiento de un marco normativo integrado para IT y OT.

• Desarrollo de capacidades en ciberinteligencia y estrategias de defensa activa.

• Fortalecimiento de la colaboración público-privada y fomento del I+D en ciberseguridad

V. Impacto esperado

• Un entorno digital más seguro y confiable.

• Mayor protección de la infraestructura crítica y los datos de los ciudadanos.

• Estímulo para la innovación tecnológica y el crecimiento económico sostenible.

El Foro Nacional de Ciberseguridad establece las bases para transformar los desafíos digitales en oportunidades estratégicas para Chile. Las propuestas integrales y el enfoque colaborativo presentado posicionan al país en un camino hacia una mayor resiliencia y liderazgo en ciberseguridad, protegiendo tanto a los ciudadanos como a los sectores críticos en un mundo cada vez más interconectado.

→Bibliografía

Las siguientes fuentes de información fueron utilizadas en la redacción de este documento:

• Ley Marco de Ciberseguridad 21.663 BNC. (2024). Ministerio del Interior y Seguridad Pública. https://www.bcn.cl/leychile/navegar?idNorma=1202434

• Foro Nacional de Ciberseguridad. Documentos de investigación https://forocyber.cl

• ISO 27001: https://www.iso.org/es/contents/data/standard/08/84/88435.html

• ISO 22237, https://www.iso.org/es/contents/data/standard/08/22/82250.html

• ISO 22301, https://www.iso.org/es/contents/data/standard/07/51/75106.html

• Decreto273, https://www.bcn.cl/leychile/navegar?idNorma=1185563

• ISO 27035, https://www.iso.org/standard/78973.html

• Decreto N ° 71, "Promulga enmiendas al anexo del Convenio Internacional para la Seguridad de la vida humana en el mar (SOLAS 1974) y el Código Internacional para la protección de los buques y de las instalaciones portuarias PBIP, adoptadas por la conferencia de los gobiernos contratantes de dicho convenio". https://www.directemar.cl/directemar/site/docs/20220616/20220616102711/codigo_pbip_version__cl_14_6_2022_rrt_caa.pdf

• Circular Marítima Directemar O-75/006 de fecha 08.06.2023, "Establece disposiciones relativas a la implementación de medidas de seguridad de la información y protección cibernética por parte de buques, instalaciones portuarias y compañías en el marco de la gestión de riesgos cibernéticos marítimos". https://www.directemar.cl/directemar/site/docs/20230616/20230616135407/o75_00_6_publ.pdf

• "Directrices sobre la gestión de los riesgos cibernéticos marítimos", Comité de la Organización Marítima Internacional, MSC-FAL.1/Circ.3 del 05.JUL.2017.

• Dimensión 1: Política y Estrategia de Seguridad Cibernética https://www.directemar.cl/directemar/site/docs/20220707/20220707162353/directri ces__gestion_de_riesgos_ciberneticos_maritimos.pdf

• "Gestión de los riesgos cibernéticos marítimos en los sistemas de gestión de la seguridad". Anexo 10, Resolución de la Organización Marítima Internacional IMO, MSC.428(98) del 16.JUN.2017. https://www.directemar.cl/directemar/site/docs/20220707/20220707160512/resolucion_omi_ciberseguridad.pdf

DIMENSIÓN 2:

Cultura cibernética y Sociedad

Moderadores:

Alexander Vianney Padilla, Angel Quiroz Chávez, Carlos Montoya, Constanza Herrera Pizzoleo, Emilio Donoso, Mary Cruz Rosas, Mauricio Castillo, René Valdez Mena, Rodrigo Pérez Galaz, Rodrigo Pérez Silva, Sebastián Zuloaga Araya.

El presente documento busca poder entregar los resultados del trabajo realizado por los moderadores y participantes del Dominio 2 – Cultura cibernética y sociedad realizado desde Abril a Octubre del 2024, y con actualización a Marzo del 2025.

Esperamos que este documento sirva de guía para entender las necesidades que se pudieron levantar, y que las iniciativas identificadas y propuestas puedan ser ejecutadas en pro de cuidar a cada ciudadano y al país, posicionando a Chile como un modelo a seguir en materias de Seguridad de la Información, Ciberseguridad, Continuidad del Negocio, y, por su puesto, Protección de datos y Privacidad.

Atentamente;

- **Constanza Herrera Pizzoleo**
- **Rodrigo Pérez Galaz**
- **Mary Cruz Rosas**
- **Angel Quiroz Chávez**
- **Mauricio Castillo**
- **René Valdez Mena**
- **Alexander Vianney Padilla**
- **Carlos Montoya**
- **Rodrigo Pérez Silva**
- **Sebastián Zuloaga Araya**
- **Emilio Donoso**

Y todos quienes participaron activamente del foro y reuniones de trabajo.

Foro Nacional de Ciberseguridad

→Contexto del Foro

Tal como lo indica en su página web https://www.forociber.cl/sobre-el-foro, esta es una iniciativa de innovación en generación de políticas públicas al alero del Senado y con la participación de expert@s. Que permitirá canalizar inquietudes y fomentar la colaboración en el ámbito de la ciberseguridad en Chile. Este foro se convierte en un espacio donde expert@s se reúnen para discutir, compartir conocimientos y promover medidas que fortalezcan nuestra seguridad en línea. El Foro Nacional de Ciberseguridad invita a académicos, profesionales, empresas y organizaciones interesados en la ciberseguridad a unirse a nuestro esfuerzo. Juntos, podemos fortalecer la seguridad en línea, proteger los derechos digitales y promover un ciberespacio confiable y generar soluciones. El objetivo principal del Foro Nacional de Ciberseguridad es promover la colaboración entre diferentes sectores para mejorar la ciberseguridad en Chile. Trabajamos en estrecha colaboración con expertos, legisladores y la comunidad en general para fortalecer la ciberseguridad y contribuir a la transformación digital del país.

→Objetivos del foro nacional de ciberseguridad

1. Crear un entorno permanente de colaboración público-privada donde compartir y generar conocimiento sobre las oportunidades y los desafíos para la seguridad en el ciberespacio.

2. Proponer iniciativas a los poderes Ejecutivo y Legislativo, para la potenciación y creación de sinergias público-privadas en materia de ciberseguridad y/o ciberdefensa, así como en la Transformación Digital del Estado.

3. Analizar, revisar, comentar y proponer anteproyectos de ley, patrocinados por un parlamentario o por el Ejecutivo, que se tramiten en el Congreso Nacional, y que requieran de las opiniones fundadas de expertos en las materias relativas al ciberespacio, ciberseguridad y transformación digital.

4. Revisar, evaluar y proponer actualizaciones a la Política Nacional de Ciberseguridad.

5. Contribuir a la identificación de las necesidades de la industria y de los centros de investigación en lo que se refiere a ciberseguridad.

6. Promover la I+D+i y la industria de la ciberseguridad nacional.

7. Canalizar y formular propuestas sobre el marco regulatorio y normativo con incidencia sobre la ciberseguridad, considerando asimismo otras disciplinas relacionadas que debieran armonizarse entre sí, como es la Transformación Digital del Estado.

8. Apoyar a la futura Agencia Nacional de Ciberseguridad en calidad de órgano consultivo.

9.Impulsar la realización proactiva de estudios e informes sobre tecnologías nuevas y emergentes y analizar su impacto en la ciberseguridad nacional y en la transformación digital del país.

10. Idear iniciativas que promuevan una cultura Nacional de Ciberseguridad.

11. Promover la proyección y participación de Chile en Latinoamérica en materia de ciberseguridad, ciberdefensa y transformación digital.

12. Patrocinar con su sello actividades de ciberseguridad a nivel nacional e internacional, en especial las actividades a realizar durante octubre de cada año en el mes de la Ciberseguridad (Ley N° 21.113).

→DIMENSIÓN 2: CULTURA CIBERNÉTICA Y SOCIEDAD

Objetivo: Mantener una cultura de Ciberseguridad responsable, basándose en el nivel de riesgos en la sociedad, nivel de confianza en los servicios de internet, gobierno en línea, y servicios comerciales en línea, y el conocimiento de los usuarios sobre la protección de información personal en línea. Además, se busca explorar la existencia de mecanismos de denuncia que operan como canales para que los usuarios denuncien la ciberdelincuencia. Finalmente revisar el rol de los medios de comunicación y redes sociales en el perfilado de valores, actitudes y comportamiento en ciberseguridad.

Esta dimensión, abarca los siguientes factores:

D2: Cultura Cibernética y Sociedad

- D2.1. Mentalidad de ciberseguridad
- D2.2. Confianza y seguridad en los servicios en línea
- D2.3. Comprensión del usuario de la protección en línea de la información personal
- D2.4. Mecanismos de notificación
- D2.5. Plataformas en línea y medios de comunicación

En la última revisión del modelo CMM (Cybersecurity Capacity Maturity Model for Nations), se presentó que los cinco factores tienen una madurez de tres, destacando el crecimiento en los factores 2.3, 2.4, y 2.5, donde en 2016 no había evaluación puesto que no existían avances en éstos.

Por esto mismo, como equipo moderador de esta dimensión, hemos podido rescatar los siguientes resultados que representan la opinión, no solo de los especialistas que participaron activamente en el foro, sino que, a través de distintas encuestas o consultas realizadas por distintos medios, y, a su vez, las necesidades detectadas.

→D2.1. Mentalidad de ciberseguridad

Como parte del factor de Mentalidad de ciberseguridad, hemos detectado que la ciudadanía identifica como parte del enfoque negativo sobre cómo se aborda la tecnología, el desconocimiento sobre lo que se comparte en dispositivos tecnológicos, compartiendo datos personales, ubicaciones, fotos, etc. Entregando dicha información como parte del precio de utilizar algo gratis. Poco se habla de leer, por ejemplo, los términos y condiciones de cada registro, descarga, uso o licencia, y menos de entender éstos, exponiendo a la ciudadanía a exponerse inseguramente, en el ciberespacio.

Si esto mismo lo llevamos a los dispositivos IoT, la sensación de inseguridad crece, puesto que un usuario que se acerca a la tecnología no es capacitado en los riesgos que puede enfrentar al utilizar este tipo de dispositivos, por lo que vemos necesario poder generar una cultura de riesgos de ciberseguridad que aborde estos desafíos de forma clara y entendible para la ciudadanía en general, y no solo enfocado en usuarios tecnológicos.

Si pensamos en la ingeniería social la preocupación es mayor, cada día vemos como los ciberdelincuentes buscan nuevas formas más convincentes de hacer caer a las personas en sus redes, tomando la tecnología como un aliado para realizar este tipo de engaños. Si vemos las campañas que existen de forma pública, podemos inferir que estás no presentan la intención de que los ciudadanos puedan identificar estas formas de ataque y la adopten en su día a día, sino que finalmente causan el efecto contrario, dado el nivel de complejidad y tecnicismos usados, aparte de no alcanzar a más público como otro tipo de campañas, por ejemplo, las radiales o de televisión, donde si podría existir un mayor alcance e interés.

Pero no todo es negativo, ante lo expuesto identificamos la necesidad urgente de poder enfocar a la ciudadanía en su higiene digital, presentando algunos tips, reales y con lenguaje más cercano, y a través de los medios de comunicación, integrando a los ciudadanos e invitándolos a comprender que la tecnología si es usada con responsabilidad y con precaución, puede ser un gran aliado.

Iniciativas identificadas:

- Capacitaciones, cápsulas, y guías que permitan a la ciudadanía entender que es Higiene digital, que les afecta y como resguardarla, integrando a los medios de comunicación para llegar a más personas.

- Campañas, cápsulas y guías que permitan a la ciudadanía entender los distintos tipos de ataques que podrían afectarles, de forma cercana y amigable, para concientizar de forma segura.

- Resguardar las comunicaciones cuando alguna entidad se vea afectada con algún incidente de seguridad, evitando una percepción negativa, y, a su vez, promover las características, iniciativas, e implementaciones que refuercen el compromiso con resguardar y proteger la información de los ciudadanos y el país.

- La complejidad técnica debe reducirse en estas iniciativas, utilizando un lenguaje accesible y cercano.

→D2.2. Confianza y seguridad en los servicios en línea

Para el caso del factor Confianza y seguridad en los servicios en línea, las necesidades abundan en que cada vez son más utilizados los canales digitales, tanto de entidades públicas como privadas, pero cada vez existe más desconfianza en ellos, esto es porque se ven más noticias de ataques en las instituciones financieras o en los servicios del gobierno, que campañas que eduquen para evitar esto, generando una publicidad negativa en dichos servicios.

Además, se identifica que las fake news y la desinformación forman parte del día a día, existiendo también, una falta en proteger la veracidad de la información que se comparte y que está dispuesta al consumo de las personas, generando un rechazo en querer utilizar estos servicios puesto que se termina por creer que lo falso es verdadero. Para esto, proponemos robustecer los canales comunicacionales, permitiendo generar distintas cápsulas informativas enfocadas en potenciar los servicios en línea, presentando las bondades de éstos y como pueden apoyar en las necesidades de cada uno de los chilenos. En la parte tecnológica, vemos la necesidad de resguardar la clave única, protegiéndola de acceso indebidos o netamente fraude a través de suplantación de identidad, quizás, una mejora significativa, sería agregar un segundo factor de autenticación, ya sea por validación con el número de documento, un código de identificación, o incluso biometría.

Iniciativas identificadas:

- Campañas en medios de comunicación para identificar las fake news, fake portal, o fake promotions, donde se busca que la ciudadanía esté atenta a éstos, buscando identificar qué información es real y cual no, al igual que portales web, promociones, ventas, etc. Y evitar caer en un fraude que les pueda afectar, por ejemplo, con una promoción falsa que les capture los datos bancarios y los usen para fraude.

- Integrar un MFA para la clave única, idealmente con biometría o un OTP seguro. Además, fortalecer la seguridad lógica de las integraciones con la clave única o los sistemas que la utilizan, evitando exfiltración de datos o robo de información sensible, incluso, una suplantación de identidad.

- Resguardar las comunicaciones cuando alguna entidad se vea afectada con algún incidente de seguridad, evitando una percepción negativa, y, a su vez, promover las características, iniciativas, e implementaciones que refuercen el compromiso con resguardar y proteger la información de los ciudadanos y el país.

→D2.3. Comprensión del usuario de la protección en línea de la información personal

Siguiendo en esta línea, para el caso del factor Comprensión del usuario de la protección en línea de la información personal, hemos detectado una brecha importante asociada en reconocer el valor de la información personal y, sobre todo, los derechos de los ciudadanos en materias de privacidad.

En el caso de entidades privadas, se ha notado un incremento en la necesidad de proteger la información, y en empresas reguladas, la opción de ejercer los derechos ARCO+P (Acceso, Rectificación, Cancelación, Oposición y Portabilidad)) a través de distintos canales, pero aún es débil, ya que son procesos que no están generados en su totalidad o simplemente, aún ni siquiera existen.

Si pensamos que en el mundo privado y regulado se da este escenario, la ciudadanía siente que en las entidades públicas no existen siquiera, dada la cantidad de exposición de la información en sistemas inseguros o que están quedando obsoletos.

Para poder solventar esto, vemos necesario considerar un mayor presupuesto enfocado en renovación tecnológica en el Estado, pero también, mejorando los procesos de selección, tanto del personal como de los proveedores, mayores auditorías a dichos procesos, y transparentando los resultados de estos, sabemos que este cambio no será en el corto plazo, pero si, que son necesarios para recuperar la confianza de los ciudadanos.

Para el caso de las entidades privadas, entendemos que, si contamos con una política nacional robusta, con metodologías y procesos claros, y que deban considerarse en el país, no solo en el Estado, obligará a éstas a adherirse y actualizarse, entregando también, un incremento en la confianza de los chilenos en éstas.

Iniciativas identificadas:

- Considerar un mayor presupuesto para robustecer, tanto técnicamente como en personas, para renovación tecnológica del Estado.

- Robustecer la concientización a la ciudadanía en materias de sus derechos y protección de datos, sobre todo, los ARCO+P, tanto a nivel Estado como a nivel regulatorio, bajo las leyes de Chile, para el privado.

- Campañas comunicaciones, integrando los medios de comunicación, para llegar a más personas.

→D2.4. Mecanismos de notificación

En el caso del factor de Mecanismos de notificación, vemos la necesidad de contar con un proceso claro, estandarizado, probado y comunicado de forma pública, de cómo se deben notificar los incidentes de seguridad de la información y ciberseguridad, potenciando las entidades que se harán cargo de recibir éstas, dar una primera guía, y ser capaz e derivar a las fuerzas de seguridad de correspondan, seguir el ejemplo de INCIBE presentara grandes oportunidades para este factor, un número de teléfono fácil y cercano, un correo electrónico, o un formulario web ayudarán a incrementar incluso los demás factores de este dominio. Pero también, contar con un canal presencial que preste ayuda, incluyendo psicológica, permitirá a los ciudadanos acercarse aún más en los cuidados y en el objetivo final de esta dimensión.

Iniciativas identificadas:

- Generar un proceso claro y comunicado de cómo se debe realizar un reporte de incidente de Seguridad de la Información y Ciberseguridad, tanto para entidades públicas, como las entidades privadas y, sobre todo, a la ciudadanía, considerando cuando ellos han sido víctima de alguno.

• Contar con canales de denuncia cercanos, un numero de 3 o 4 dígitos, un portal, un correo, y sobre todo, una oficina física donde se pueda canalizar este tipo de situaciones.

• Contención psicológica, tanto para los ciudadanos que han pasado por algún ciber incidente, como para los equipos TI que tienen que contener o son parte de los afectados, considerando apoyo psicológico, contención emocional, apoyo en actividades que puedan generar ayuda en general.

→D2.5. Plataformas en línea y medios de comunicación

Finalmente, para el caso del factor Plataformas en línea y medios de comunicación, se conecta todo lo indicado en los factores anteriores, existe una deuda importante como país de poder comunicar, de forma clara, precisa, y concisa, los riesgos de seguridad de la información y ciberseguridad, y como abordar éstos para evitar ser una víctima si alguno se materializa, reforzamos la necesidad de realizar campañas comunicacionales enfocadas en la ciudadanía, utilizando los medios de comunicación más utilizados por los chilenos, buscando tener el mayor alcance posible. Pero también, capacitando a los funcionarios de los sectores públicos y privados, para poder guiar cuando se requiera.

Iniciativas identificadas:

• Considerar dentro del presupuesto anual, la generación de campañas, informativos, capsulas, etc., enfocadas en sector público y privado, de lo propuesto en los factores anteriormente descritos.

• Refuerzo de campañas comunicacionales cercanas para la ciudadanía y para los funcionarios de los sectores públicos y privados.

→*Frameworks* y Normativa Legal vigente aplicable

Para el desarrollo de las iniciativas propuestas anteriormente, se recomienda considerar los siguientes frameworks y normativa legal vigente aplicable, que permitirán sustentar la necesidad de aplicar las medidas a través de metodologías probadas y, a su vez, con un respaldo legal que permitirá, tanto a las instituciones del servicio público como a privados, tener el respaldo legal necesario.

→NIST CSF 2.0

El CSF fue diseñado para que sea utilizado por organizaciones de todos los tamaños y sectores, lo que incluye a la industria, el gobierno, el mundo académico y las organizaciones sin fines de lucro, sin importar el nivel de madurez de sus programas de seguridad cibernética. El CSF es un recurso fundamental que se puede adoptar voluntariamente y a través de políticas y mandatos gubernamentales.

La taxonomía del CSF y las normativas, directrices y prácticas referenciadas no son específicas de un país, y las versiones anteriores del CSF fueron aprovechadas con éxito por diversos gobiernos y otras organizaciones tanto dentro como fuera de los Estados Unidos.

El CSF se debe utilizar junto con otros recursos (p. ej., marcos, normas, directrices, prácticas principales) para gestionar mejor los riesgos de seguridad cibernética e informar la gestión general de los riesgos de la tecnología de la información y las comunicaciones (ICT) a nivel empresarial. El CSF es un marco flexible que se ha diseñado para su uso por parte de todas las organizaciones, sin importar su tamaño.

Las organizaciones seguirán teniendo riesgos únicos incluidas las diferentes amenazas y vulnerabilidades- y tolerancias al riesgo, así como objetivos y requisitos de misión únicos. Por lo tanto, los enfoques de las organizaciones para gestionar los riesgos y sus implementaciones del CSF variarán.

Imagen 1. Funciones del NIST CSF 2.0

→Función Proteger (PR)

En esta función se encuentra la categoría "Concienciación y Capacitación – PR.AT" la cual permite proporcionar a las personas concienciación y capacitación en seguridad cibernética para que puedan realizar sus tareas relacionadas con la seguridad cibernética. Dentro de la misma se encuentran las siguientes subcategorías, que permitirán ser utilizadas para dar cumplimiento a las iniciativas y necesidades identificadas.

Concienciación y Capacitación – PR.AT

- **PR.AT-01:** Se sensibiliza y capacita al personal para que disponga de los conocimientos y habilidades necesarios para realizar tareas generales teniendo en cuenta los riesgos de seguridad cibernética.

- **PR.AT-02:** Se sensibiliza y capacita a las personas que desempeñan funciones especializadas para que posean los conocimientos y aptitudes necesarios para realizar las tareas pertinentes teniendo en cuenta los riesgos de seguridad cibernética

Para el caso de la categoría "Gestión de identidades, autenticación y control de acceso (PR.AA)", donde se indica que el acceso a los activos físicos y lógicos se limita a los usuarios, servicios y hardware autorizados y se gestiona de forma proporcional al riesgo evaluado de acceso no autorizado, se deben considerar la totalidad de las subcategorías.

- **PR.AA-01:** La organización gestiona las identidades y credenciales de los usuarios, servicios y equipos autorizados

- **PR.AA-02:** Las identidades están comprobadas y vinculadas a credenciales basadas en el contexto de las interacciones

- **PR.AA-03:** Los usuarios, servicios y hardware están autenticados o

- **PR.AA-04:** Las afirmaciones de identidad se protegen, transmiten y verifican

- **PR.AA-05:** Los permisos de acceso, los derechos y las autorizaciones se definen en una política, se gestionan, se aplican y se revisan, e incorporan los principios de privilegio mínimo y separación de funciones

- **PR.AA-06:** El acceso físico a los activos se gestiona, supervisa y aplica de forma proporcional al riesgo

Para el caso de la categoría "Seguridad de los datos (PR.DS)", donde los datos se gestionan de forma coherente con la estrategia de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de la información, aplican también todas las subcategorías.

- **PR.DS-01:** La confidencialidad, la integridad y la disponibilidad de los datos en reposo están protegidas.

• **PR.DS-02:** La confidencialidad, la integridad y la disponibilidad de los datos en tránsito están protegidas.

• **PR.DS-10:** La confidencialidad, la integridad y la disponibilidad de los datos en uso están protegidas.

• **PR.DS-11:** Se crean, protegen, mantienen y comprueban copias de seguridad de los datos

→Función Responder (RS)

En esta función se encuentra la categoría "Notificación y comunicación de la respuesta al incidente – RS.CO" la cual entrega una guía donde, las actividades de respuesta se coordinan con las partes interesadas internas y externas, según lo exijan las leyes, las normativas o las políticas.

Notificación y comunicación de la respuesta al incidente – RS.CO

• **RS.CO-02:** Se notifican los incidentes a las partes interesadas internas y externas.

• **RS.CO-03:** La información se comparte con las partes interesadas internas y externas designadas.

→Función Recuperar (RC)

En esta función se encuentra la categoría "Ejecución del Plan de Recuperación de Incidentes (RC.RP)" la cual entrega una guía donde, se realizan actividades de restauración que garantizan la disponibilidad operativa de los sistemas y servicios afectados por incidentes de seguridad cibernética.

Puntualmente, en esta categoría, se rescata la siguiente subcategoría:

• **RC.RP-06:** Se declara el fin de la recuperación del incidente sobre la base de criterios y se completa la documentación relacionada con el incidente Para el caso de la categoría "Comunicación de la recuperación del incidente (RC.CO)" que indica las acciones para coordinar las actividades de restauración con las partes internas y externas, se deben considerar todas las subcategorías.

• **RC.CO-03:** Las actividades de recuperación y los progresos en el restablecimiento de las capacidades operativas se comunican a las partes interesadas internas y externas designadas.

• **RC.CO-04:** Las actualizaciones públicas sobre la recuperación del incidente se comparten mediante el uso de métodos y mensajes aprobados.

Sin desmedro de lo anteriormente descrito, es siempre recomendable tomar el CSF completo, evaluarlo, y tomar las acciones correspondientes, dado que finalmente todas éstas ayudarán en mantener una ciber resiliencia en el país.

→ISO 27001

La norma ISO 27001 es un estándar internacional que establece los requisitos para gestionar la seguridad de la información de una organización. Su objetivo es proteger los datos y la información de la empresa, evitando su pérdida o robo.

Beneficios de la norma ISO 27001

- Minimizar los riesgos de seguridad de la información
- Minimizar los riesgos de sanciones
- Confianza de proveedores y clientes
- Cumplimiento de los requisitos legales y reglamentarios
- Mejorar la competitividad y la imagen de la organización

Qué incluye la norma ISO 27001

- Definición del sistema de gestión de seguridad de la información
- Accesibilidad a la información si es necesario
- Mantenimiento regular y mejora de los sistemas de gestión
- Evaluación del riesgo
- Aplicación de los controles necesarios para mitigar o eliminar los riesgos

La norma ISO 27001 se recomienda a todas las empresas, independientemente de su tamaño o sector.

→ISO 27002

La norma ISO 27002 es un estándar internacional que proporciona directrices para la implementación de controles de seguridad de la información. A diferencia de la norma ISO 27001, que se centra en los requisitos para establecer un Sistema de Gestión de la Seguridad de la Información (SGSI), la norma ISO 27002 actúa como un complemento a la norma ISO 27001. Un estándar que ofrece un conjunto detallado de directrices y mejores prácticas para implementar los controles de seguridad identificados en el Anexo A de la ISO 27001. Es una norma clave como recurso detallado para las organizaciones que buscan una guía sobre las mejores prácticas en seguridad de la información.

Controles

Controles Organizacionales

Estos controles tienen como objetivo principal proporcionar un esquema operativo para la seguridad de la información. Se enfocan en:

- Definición de estructuras de gobernabilidad y roles.
- Establecimiento de políticas claras.

- Fomento de una cultura de seguridad de la información.
- Asegurar el cumplimiento regulatorio.
- Gestión proactiva de riesgos.
- Adaptabilidad ante el cambio.
- Incentivar una búsqueda constante de mejora.

Controles de Personas:

Estos controles reconocen la importancia del factor humano en la seguridad de la información. Se centran en:

- Concientización y formación del personal.
- Establecimiento de procesos de reclutamiento seguros.
- Definición clara de responsabilidades en la contratación.
- Evaluaciones periódicas y disciplina en caso de incumplimientos.
- Protocolos de terminación de empleo que garantizan la continuidad de la seguridad.

Controles Físicos:

La seguridad no solo es digital, y estos controles se encargan de la protección tangible.

Abordan:

- Salvaguarda de equipos y dispositivos.
- Protección de medios de almacenamiento.
- Seguridad de las instalaciones físicas.
- Medidas preventivas contra incidentes, ya sean naturales o intencionados.

Controles Tecnológicos:

Con un enfoque en la infraestructura tecnológica, estos controles cubren:

- Procesos seguros desde el diseño hasta la implementación de sistemas.
- Mantenimiento y configuración de redes.
- Monitoreo constante.
- Análisis y pruebas periódicas.
- Procedimientos de auditoría y recuperación en caso de incidentes.

→Ley 21.663 – Ley Marco de Ciberseguridad

La Ley 21.663, también conocida como Ley Marco de Ciberseguridad, establece directrices para prevenir, detectar y responder a incidentes cibernéticos. Esta ley se aplica a sectores críticos del país, como las telecomunicaciones, la energía, el transporte, la salud y las finanzas.

La Ley 21.663 se basa en principios como: Control de daños, Cooperación con la autoridad, Coordinación, Seguridad en el ciberespacio.

Esta ley regula la ciberseguridad en Chile, protegiendo sistemas de información y infraestructuras críticas en sectores públicos y privados.

- Promueve políticas, auditorías y capacitación
- Fortalece la resiliencia digital y continuidad de servicios
- Establece la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad
- Establece los requisitos mínimos para la prevención, contención, resolución

La Ley 21.663 afecta a los organismos públicos, empresas del estado, municipalidades y a todas las empresas privadas que prestan servicios calificados como esenciales.

→Ley 21.719 – Regula la protección y el tratamiento de datos personales

El objetivo principal de la Ley 21.719 de Chile es establecer un marco normativo que garantice la protección de los datos personales y la privacidad de los ciudadanos en un mundo cada vez más digitalizado. Busca regular cómo se recopilan, procesan, almacenan y transfieren los datos personales, asegurando que estos se manejen de forma ética, segura y conforme a los derechos de las personas. En términos prácticos, la ley pretende equilibrar el desarrollo tecnológico y económico con el respeto p

or la privacidad, otorgando a los ciudadanos mayor control sobre su información personal y fomentando la transparencia en el uso de dichos datos por parte de las organizaciones. También establece un mecanismo de supervisión mediante la creación de la Agencia de Protección de Datos Personales para hacer cumplir estas regulaciones.

En resumen, los puntos clave que abarca son:

- **Principios fundamentales:** La ley establece principios como finalidad, proporcionalidad, seguridad y confidencialidad en el tratamiento de datos personales.

- **Derechos de los titulares:** Incluye derechos como acceso, rectificación, supresión, oposición, portabilidad de datos y revocación del consentimiento.

- **Tratamiento de datos:** Requiere consentimiento informado y explícito, con regulaciones específicas para datos sensibles, biométricos y de menores.

• **Transferencias internacionales:** Solo se permite hacia países con protección adecuada o bajo condiciones específicas.

• **Creación de la Agencia de Protección de Datos Personales:** Este organismo autónomo supervisará el cumplimiento de la ley y garantizará la protección de los derechos de privacidad.

• **Sanciones:** Las infracciones pueden ser sancionadas con multas significativas, dependiendo de su gravedad.

→Conclusión

Si como ciudadanos logramos generar una conciencia de los riesgos y las necesidades que nos enfrentamos día a día al navegar en el ciberespacio sin duda seríamos mas precavidos sobre la información que entregamos, como la entregamos, y a quien la entregamos.

El hecho de que en Chile se considere dentro de la agenda país la Ciberseguridad, nos posiciona entre los lideres en Latinoamérica, y si considera también, la oportunidad de que la misma ciudadanía a través de distintos especialistas, la posibilidad de que puedan aportar al país con su visión en estas materias, ayuda a generar finalmente un Chile más ciberseguro.

Las necesidades identificadas en este documento son el fiel reflejo de esto, de la preocupación de la ciudadanía y de como desean poder contar con un apoyo más robusto, desde el Gobierno hasta cada uno de los chilenos.

De estas necesidades, se logró poder rescatar distintas iniciativas correspondientes a la Dimensión 2 - Cultura cibernética y Sociedad, donde cada una de estas busca ser un aporte para el plan próximo que Chile desea abordar para mejorar.

Además de estas iniciativas, se presenta una guía de marcos de trabajo (Frameworks) y su relación con las dos (2) Leyes promulgadas durante 2024 y que son el pilar fundamental para realizar esta mejora en la postura de seguridad de la información, ciberseguridad y continuidad en el país.

Esperamos que este documento cumpla el objetivo de hacer a Chile más ciberseguro.

DIMENSIÓN 3:

Desarrollando conocimiento y capacidades en ciberseguridad

Moderador:

Karin Quiroga Suazo
Romina Torres

Este documento ha sido preparado para el Foro Nacional de Ciberseguridad. Dimensión 3, Desarrollando conocimiento y capacidades en ciberseguridad. Factor 3.3, Formación profesional en ciberseguridad.

Autora: **Karin Quiroga Suazo. Alianza Chilena de Ciberseguridad.**

Colaboradores y participantes del Foro: **Lidia Herrera Mateluna, Jaime Gómez González, Paola Vera Toledo, Margarita Vargas Martinez, Rosa María Fuentes Valdebenito.**

Fecha de publicación: Noviembre 2024.

Equipo de Redacción Factor 3.4, Investigación e Innovación en Ciberseguridad.

Romina Torres, Julio Fenner, Carlos Manzano, Nicolás Boettcher, Sebastián Berríos, Freddy Grey, Paolo Norambuena, Nicolás Matus, Camilo Vásquez, Pedro Pinacho, Francisco Alonso, Gustavo Ortiz, Marcos Vejar.

Fecha de publicación: Octubre 2024.

→Introducción

El avance tecnológico sin precedentes de las últimas décadas ha impulsado la creación de nuevos desafíos en el ámbito de la ciberseguridad. La transformación digital, el Internet de las Cosas (IoT), la Inteligencia Artificial (IA) y la conectividad global han abierto la puerta a innumerables oportunidades, pero también han creado un panorama de amenazas que requiere una respuesta sofisticada y rápida. En este contexto, la formación y el desarrollo de profesionales en ciberseguridad se ha convertido en una necesidad crítica para enfrentar los desafíos que surgen de un entorno digital cada vez más complejo.

Desde ataques de ransomware hasta brechas de datos que exponen información sensible, los riesgos son innumerables, lo que exige no sólo la adopción de tecnologías avanzadas, sino también la disponibilidad de profesionales capacitados para gestionar y mitigar estas amenazas. Sin embargo, la creciente demanda de expertos en ciberseguridad ha evidenciado una significativa escasez de talento en esta área, tanto en Chile como a nivel global.

Uno de los principales desafíos que enfrenta el campo de la ciberseguridad es la falta de personal capacitado. Se estima que, a nivel global, hay un déficit de más de 3.5 millones de profesionales en ciberseguridad. En Chile, la Política Nacional de Ciberseguridad 2023-2028 estima que se necesitarán al menos 28,000 especialistas para satisfacer las necesidades del sector público y privado. (Ministerio del Interior y Seguridad Pública, 2023).

Además, el desarrollo de la Inteligencia Artificial ha transformado de manera significativa múltiples sectores, desde la industria manufacturera hasta la atención sanitaria, y continúa avanzando rápidamente en áreas clave como la ciberseguridad. La IA, definida como la capacidad de las máquinas para realizar tareas que generalmente requieren inteligencia humana, ha mostrado su potencial para mejorar la detección, respuesta y prevención de amenazas cibernéticas, áreas en las que la seguridad de la información es cada vez más crítica.

El vínculo entre IA y ciberseguridad está marcado por la creciente capacidad de las herramientas de IA para monitorear, detectar y responder a ciberamenazas en tiempo real. La integración de IA en soluciones de ciberseguridad ha permitido que las organizaciones puedan gestionar volúmenes masivos de datos que serían imposibles de procesar mediante métodos tradicionales. Además, la IA tiene la capacidad de identificar patrones en grandes conjuntos de datos, lo que permite detectar amenazas avanzadas que podrían pasar desapercibidas con las herramientas convencionales o involucrar una gran cantidad de recursos para su procesamiento.

Si bien los desafíos en la formación de profesionales en ciberseguridad son significativos, también existen oportunidades importantes. La colaboración entre gobiernos, el sector privado y las instituciones académicas es clave para garantizar que los programas formativos estén alineados con las demandas de las distintas industrias. En este sentido, la creación de alianzas público-privadas puede ser una estrategia eficaz para fomentar la innovación y mejorar la calidad de la educación y formación en ciberseguridad.

→Foro Nacional de Ciberseguridad

El Foro Nacional de Ciberseguridad de Chile es una plataforma creada para promover la colaboración entre los sectores público, privado y académico con el objetivo de fortalecer la ciberseguridad del país. Este foro nace al alero de mesa de ciberseguridad de la Comisión Desafíos del Futuro, Ciencia, Tecnología e Innovación del Senado de Chile, cuando el año 2022 se construyó el informe "Ciberseguridad para Chile, un camino a recorrer". Este documento que generó una serie de recomendaciones y contó con la participación de 140 especialistas provenientes de la academia, la industria, servicios públicos, Policías, Fuerzas Armadas, organizaciones civiles y otros profesionales focalizados en temas atingentes a ciberseguridad, transformación digital y políticas públicas.

El Foro se basa en el **MODELO DE MADUREZ DE CIBERCAPACIDADES PARA NACIONES (CMM) DE LA UNIVERSIDAD DE OXFORD.** Considera 5 **dimensiones** que cubren la amplitud de la capacidad nacional de ciberseguridad valuada por el CMM. A su vez, cada dimensión está compuesta de **Factores** que describen lo que significa poseer capacidad de ciberseguridad. Luego encontramos los **Aspectos,** que corresponden a un método organizativo para dividir los indicadores en grupos más pequeños y que sean más fáciles de comprender. Finalmente se encuentran los **Indicadores,** que representan la parte más básica de la estructura de CMM.

Figura 1. Dimensiones del Modelo CMM.
Fuente: Foro Nacional de Ciberseguridad

→ DIMENSIÓN 3: DESARROLLANDO CONOCIMIENTO Y CAPACIDADES EN CIBERSEGURIDAD

La tercera dimensión revisa la disponibilidad, calidad y aceptación de programas para varios grupos de partes interesadas, incluido el gobierno, el sector privado y la población en general, y se relaciona con programas de concienciación sobre ciberseguridad, programas oficiales educativos en ciberseguridad, así como programas de formación profesional. Posee los siguientes factores.

- **Factor D 3.1 : Desarrollo de Concientización en Ciberseguridad**
- **Factor D 3.2 : Educación en ciberseguridad**
- **Factor D 3.3 : Formación profesional en ciberseguridad**
- **Factor D 3.4 : Investigación e innovación en ciberseguridad**

a. Factor D 3.3: Formación profesional en ciberseguridad

La Dimensión 3 del Foro Nacional de Ciberseguridad de Chile, enfocada en el desarrollo de conocimiento y capacidades en ciberseguridad, busca mejorar la formación, educación y habilidades en ciberseguridad para los diferentes sectores e industrias. El Factor D 3.3, que se centra en la formación profesional en ciberseguridad como un palanca clave para asegurar que haya una fuerza laboral capacitada que pueda enfrentar los retos actuales y futuros en este campo, está alineado con la necesidad global de contar con más profesionales capacitados en ciberseguridad. Lo anterior, es un desafío debido a la creciente demanda y escasez de expertos. Está específicamente orientado a:

1. La disponibilidad y provisión de programas asequibles de formación profesional en ciberseguridad para construir un organismo de profesionales de ciberseguridad.

2. La reconversión profesional como motor de innovación en ciberseguridad; la reconversión de profesionales de otras áreas para cubrir la brecha de profesionales existentes aportará un valor desde la experiencia interdisciplinaria que entregarán una visión única y complementarán los nuevos desafíos que enfrentaremos en ciberseguridad. Para ello es indispensable contar con programas de formación flexibles y accesibles que permitan compatibilizar trabajo con estudio y que incluyan el reconocimiento de experiencias previas, para acelerar su proceso de aprendizaje.

3. La adopción de la formación horizontal y vertical del conocimiento en ciberseguridad y la transferencia de habilidades dentro de las organizaciones.

4. Y cómo esta transferencia de habilidades se traduce en un aumento continuo de organismos de profesionales de ciberseguridad.

El **Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM)** (Global Cyber Security Capacity Centre, 2021), sobre el cual se basa el Foro, es un marco metodológico que mide la capacidad de ciberseguridad de los países en cinco niveles de madurez para cada uno de sus factores. A continuación, se presentan los cinco niveles para el factor 3.3.

Aspecto	Start-Up	Formative	Established	Strategic	Dynamic
Provisión	Pocos o ningún programa de formación en ciberseguridad existe.	Se ha documentado la necesidad de capacitar a profesionales en ciberseguridad a nivel nacional. Se ofrece formación para el personal de TI general, pero no para profesionales dedicados a la seguridad.	Existen programas estructurados para desarrollar habilidades y formar profesionales en ciberseguridad. Se consideran marcos nacionales o internacionales al diseñar los cursos. Se ofrece certificación de seguridad profesional a nivel nacional. Existen programas para no profesionales de ciberseguridad. Iniciativas gubernamentales para retener talento podrían existir.	Se ofrecen cursos adaptados a la demanda estratégica nacional y alineados con buenas prácticas internacionales. Los programas de formación reflejan las prioridades de la estrategia de ciberseguridad. Se miden los resultados para ajustar los programas futuros.	Los sectores público y privado colaboran para ofrecer formación y crear habilidades. Los programas de educación están coordinados para desarrollar una fuerza laboral altamente capacitada. Existen incentivos para retener el talento formado dentro del país.
Adopción	La adopción de la formación en ciberseguridad por parte del personal de TI es limitada o inexistente. No hay transferencia de conocimientos entre empleados capacitados y no capacitados.	Los indicadores de adopción de cursos, seminarios y certificaciones son limitados. La transferencia de conocimientos entre empleados capacitados y no capacitados en el sector público y privado es ad hoc.	Existe un grupo de empleados certificados capacitados en ciberseguridad. Puede existir un registro nacional de estudiantes y profesionales certificados. Los procesos de revisión del programa permiten medir el progreso y la demanda de trabajadores capacitados en ciberseguridad en los sectores público y privado.	La adopción de la formación en ciberseguridad se utiliza para informar futuros programas. La coordinación de la formación en todos los sectores asegura que se satisfaga la demanda nacional de profesionales.	Los profesionales de ciberseguridad no solo satisfacen las necesidades nacionales, sino que se consulta a los profesionales nacionales en el extranjero para compartir lecciones y mejores prácticas.

Tabla 1. Niveles CMM. Factor 3.3: Formación profesional en ciberseguridad
Fuente: Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM). Traducción propia.

Según el **Reporte Ciberseguridad 2020. (Foro Nacional de Ciberseguridad de Chile. 2020). En la Dimensión 3 y el factor 3.3 Formación profesional en ciberseguridad** entre el 2016 y 2020, Chile avanzó del nivel 2 al nivel 3. Es decir, se pasó de un nivel **FORMATIVO,** donde se están desarrollando programas iniciales de capacitación, a un nivel **CONSOLIDADO,** donde se observan implementaciones, formalización de políticas y prácticas de ciberseguridad y los programas de formación ya están funcionando de forma consistente. Esto se debe principalmente a que:

1. **Se observa un incremento en la cantidad y calidad de los programas de formación en ciberseguridad alineados a estándares internacionales, como ISO y NIST.**

2. **Se visibilizan marcos de competencias y habilidades con mejores prácticas internacionales.**

3. **Se potencian los programas de certificación para profesionales del sector.**

El siguiente desafío es avanzar hacia los niveles **ESTRATÉGICO,** donde la formación está alineada con una estrategia nacional clara y luego al nivel **DINÁMICO,** donde la formación profesional en ciberseguridad es adaptativa y proactiva frente a nuevas amenazas y tecnologías emergentes.

→ IV. Benchmarking Nacional

A continuación, se realizará un levantamiento de los principales desafíos abordados en materia de formación en ciberseguridad en distintas instancias nacional para los últimos años.

a. Estrategia de Transformación Digital, Chile Digital 2035.

Destaca la **formación profesional en ciberseguridad** como una de las áreas clave para enfrentar los desafíos de la digitalización. Este plan busca capacitar a la fuerza laboral cuyas funciones están siendo reemplazadas por la transformación digital, preparándolos para nuevos roles relacionados con la seguridad digital. (Órdenes, Roberts, Rojas, & Rojas, 2023).

La Estrategia de transformación digital para Chile está sustentada en dos pilares: Chile conectado sin brechas y Chile digitalizado. Ambos, a su vez, comprenden un conjunto de iniciativas, acciones, programas y proyectos que permiten garantizar el acceso, aprovechamiento y uso adecuado de la tecnología.

Figura 2. Estrategia Chile Digital.
Fuente: Estrategia de Transformación Digital.

En el componente de ciberseguridad destaca el **Objetivo 3. Gestión del Talento, desarrollo de capacidades y de industria de ciberseguridad,** que aborda la disponibilidad y ejecución de programas de formación y educación en ciberseguridad, de alta calidad, con programas de capacitación y certificación de competencias. Este objetivo, además, mejora la colaboración entre el gobierno y la industria para asegurar que las inversiones educativas satisfagan las necesidades de educación en ciberseguridad en todos los sectores, en base a una entidad rectora con competencia en estas materias (Órdenes, Roberts, Rojas, & Rojas, 2023). Algunas de las líneas de intervención que se desprenden de este objetivo y que tributan al desarrollo profesional y formación en ciberseguridad son:

- Crear el Instituto Nacional de Ciberseguridad (INCIBER) en Valparaíso para articular la red de investigación avanzada en ciberseguridad, desarrollo de talento ciber y formación avanzada de instructores y especialistas de distintas áreas, junto al establecimiento de medios de evaluación y acreditación de competencias, organización de ejercicios nacionales y actividades de promoción y de difusión de nuevos conocimientos en ciberseguridad.

• Mejorar las ofertas educativas de ciberseguridad, estableciendo programas de formación y acreditación de competencias, de acuerdos a estándares nacionales e internacionales, para carreras técnicas y universitarias.

• Fomentar la incorporación de mujeres a carreras de ciberseguridad para hacerse cargo de la brecha de género existente.

• Incentivar la formación y retención de especialistas en ciberseguridad para apoyar al Estado, los servicios de este, y a los actores económicos en general.

• Explorar la coordinación, y los recursos para desarrollar marcos educativos de ciberseguridad mejorados, con presupuesto y gasto basado en la demanda nacional de forma dinámica y con recursos de la ley de presupuesto.

• Colaborar en ciberseguridad entre el ámbito civil y las entidades de la defensa, mediante proyectos de tecnologías duales (uso civil y militar) junto con la existencia de recursos anuales adecuados disponibles para su ejecución.

Las metas propuestas asociadas al desarrollo profesional y formación en ciberseguridad en dos de sus componentes son:

Componentes	Metas
Desarrollo de habilidades digitales	• Al menos igualar el promedio de la OCDE al 2035 en el desarrollo de habilidades digitales básicas y avanzadas. • Establecer un plan nacional de reconversión de la fuerza laboral cuyos trabajos desaparecieron por la transformación digital al 2025. • Incrementar la cantidad de profesionales en disciplinas en ciencia, tecnología, ingeniería y matemáticas (STEM) al menos igualar los niveles promedio de los países de la OCDE.
Ciberseguridad	• Creación del Instituto Nacional de Ciberseguridad y del Centro de Capacidades de Ciberseguridad de Iberoamérica al 2023. • Formación de 10.000 profesionales certificados en Ciberseguridad al 2035, donde al menos el 30% de ellos sean mujeres. • Alcanzar el 2035 una "Madurez en Ciberseguridad" cercana al Estado 5 o "Dinámico" para una nación, de acuerdo con el CMM de la Universidad de Oxford, en todos los factores con al menos evaluación Estado 4 y medido de forma externa.

Tabla 2. Metas Componentes Estrategia de Transformación Digital, Chile Digital 2035.
Fuente: Estrategia de Transformación Digital.

b. Construyendo la ciberseguridad en Chile (2023).

Documento desarrollado por la **Mesa de Ciberseguridad de la Comisión Desafíos del Futuro** con la participación de 140 expertos nacionales y 7 sub-mesas. Este documento recoge los principales desafíos y plasma las necesidades y oportunidades como país que debemos considerar en materias de ciberseguridad. Se focaliza en 7 áreas principales: **1) Ciberseguridad y Políticas Públicas. 2) Desarrollo Talento. 3) Investigación Avanzada. 4) Tecnologías Emergentes. 5) Operadores de Servicios Esenciales. 6) Desinformación en Línea. 7) Interoperabilidad e Identidad Digital.** (Biblioteca del Congreso Nacional de Chile. (n.d.))

Para **Desarrollo Talento,** involucra grandes desafíos por las brechas actuales en distintas áreas y la necesidad de contar con profesionales especializados según las nuevas normativas y estrategias en ámbitos legislativos. Los desafíos en formación se plantean en todos los niveles académicos, desde la educación secundaria, superior, capacitación y educación continua. Además, se plantea la necesidad para avanzar en el cierre de brechas en materias de la participación de mujeres en ciberseguridad y tecnología.

Este capítulo identifica 19 propuestas concretas y 6 para educación continua y formación profesional.

Propuesta	Descripción	Acciones	Impactos
12. Generación de Diplomas y Certificaciones de Competencia.	Fomentar la generación de Diplomas y Certificaciones acorde con las necesidades del ecosistema chileno.	• Generar planes de programas de certificación amplios que recojan las necesidades de instituciones tanto públicas como privadas. • Fomentar la homologación de certificaciones nacionales a estándares internacionales que puedan ser otorgadas por las instituciones de formación nacional, con las acreditaciones correspondientes. • Establecer certificaciones que permitan acreditar una competencia básica en Ciberseguridad, tendientes a incentivar carreras profesionales en Ciberseguridad en línea con las Certificaciones en Ciberseguridad Internacionales.	• Fomentar, actualizar y homologar la certificación a nivel internacional en materia de ciberseguridad a los funcionarios de las distintas instituciones (Públicas y privadas) para reducir las brechas detectadas. • Fomentar la capacitación del personal institucional en las certificaciones internacionales en Ciberseguridad. • Convertir al país en referente en ciberseguridad al generar un Certificado nacional básico (abierto a toda la población) para que se dominen tópicos básicos y dar continuidad de estudio homologado con los más altos estándares internacionales.

13. Capacitación de empresas y organismos estatales.	Mejorar el nivel general de capacitación en ciberseguridad del personal de las empresas y de los organismos estatales. Tratar la ausencia de un diagnóstico del estado de madurez en ciberseguridad. Exponer un modelo único y nacional para desarrollar el análisis de madurez.	• Realizar un catastro y diagnóstico en distintas Instituciones del nivel de ciberseguridad. Asimismo, determinar si existe personal competente o especializado para operar en la materia. • El Estado deberá patrocinar iniciativas e incentivos, promoviendo vínculos con otras instituciones (internacionales o nacionales) públicas y privadas, para acortar las brechas diagnosticadas, con el propósito de generar planes directores en capacitación sectoriales para poder cubrir las brechas. • Consolidar el ecosistema (Públicas y privadas) como promotor de mejora continua en materias de educación de ciberseguridad con foco para empresas y organismos estatales.	• Tener un catastro actualizado de las fortalezas y deficiencias de los funcionarios públicos en las distintas instituciones. • Disminución de las brechas detectadas en el diagnóstico, fomentando un ecosistema de mejora continua. • Consolidación del ecosistema (Públicas y privadas) como promotor de mejora continua en materias de educación de ciberseguridad con foco para empresas y organismos estatales.
16 - Generar la "Plataforma nacional de Ciber formación y ciber empleos– orientado a Ciberseguridad.	Ausencia de nexos eficientes para la reconversión. Exponer métodos para fomentar la reconversión.	• Realizar un estudio en conjunto con la academia y organizaciones de la sociedad, para estimar demandas y público objetivo. • El Estado patrocinará iniciativas e incentivos, a través de organismos como Sence, al objeto de establecer una bolsa nacional de empleos tecnológicos, digitales y de ciberseguridad. A lo anterior se promoverá un programa nacional de reconversión profesional a ciberseguridad. (base Corfo: Becas Capital Humano). • Generar ferias laborales con foco en reconversión laboral, de personal en retiro de fuerzas armadas, empleados públicos, mujeres y ciudadanos neuro	• Tener un estudio a nivel nacional de sectores y profesiones que podrían ser parte de un programa de educación con foco en reconversión. • Aumentar la reconversión profesional a especialistas en ciberseguridad. • Generar un sistema de capital humano para fortalecer la demanda de especialistas en Chile.

		diverso similar a como se realiza en EE. UU.	
17 - Creación del Instituto Nacional de Ciberseguridad (INCIBER)	Es necesario crear un Instituto Nacional de Ciberseguridad en Chile, como es el caso de España (con el INCIBE). El rol del INCIBER chileno será la creación de un ecosistema de ciberseguridad, cubriendo la difusión, innovación y fomento de la ciberseguridad, incluyendo el mundo académico, el mundo empresarial, los organismos del Estado y la sociedad civil organizada.	• Creación de normas nacionales de referencia para la educación de los futuros expertos en ciberseguridad en el país. Cumplir un rol articulador en la investigación y desarrollo nacional de la ciberseguridad. Establecer nexos con instituciones afines a nivel internacional. • Organizar ejercicios nacionales de ciberseguridad en conjunto con la academia para fomentar el aprendizaje en grupo de técnicas de ciberdefensa, así como detectar talentos en la materia. • Generar certificaciones nacionales en ciberseguridad (al estilo del EC-Council) en cooperación con los establecimientos de educación superior. • Generar un sistema de acreditación en ciberseguridad para cursos sobre la materia (un label de calidad: Sello INCIBER.	• Creación de un ecosistema entre el Estado, la academia y las empresas para generar un marco de cooperación en educación y difusión en ciberseguridad. • Creación de un modelo de certificación de la educación en ciberseguridad. • Mejora de la cooperación entre el mundo académico y el mundo empresarial en ciberseguridad.
18 - Crear un equivalente de la Estonian Defence League's Cyber Unit de Estonia	La Estonian Defence League's Cyber Unit es una organización que tiene como objetivo la defensa del ciberespacio del país. Incluye miembros de organizaciones estatales especialistas en ciberseguridad, así como profesionales de empresas privadas y voluntarios de la sociedad civil.	• Creación de una asociación para la defensa del ciberespacio chileno en cooperación con el mundo académico, representantes del Estado, profesionales en ciberseguridad y voluntarios de la sociedad civil. • Crear una división en el INCIBER para la gestión, la implementación y el entrenamiento de esta asociación. • Organizar ejercicios de entrenamiento a nivel internacional para los miembros de esta asociación de	• Tener una reserva nacional de especialistas en ciberseguridad para poder enfrentar cualquier escenario de ataque a nivel nacional. • Generar una cooperación entre el mundo civil y militar en ciberseguridad (Ministerio de Defensa y Ministerio a cargo de la Seguridad Pública). • Detectar y promover a talentos en ciberseguridad que no están en el sistema

		defensa del ciberespacio chileno (por ejemplo, en cooperación con Estonia u otros países de buen ranking en ciberseguridad).	tradicional de educación superior.

Tabla 3. Propuestas Proyecto Construyendo la Ciberseguridad en Chile.
Fuente: Construyendo la Ciberseguridad en Chile.

c. Hoja de Ruta de Ciberseguridad (2023)

Realizado por Microsoft Chile y el Centro de Innovación UC, este estudio busca definir y orientar una estrategia y una táctica de forma asociativa y concreta hacia el desarrollo y bienestar de Chile, incidiendo también en la política pública nacional. (Centro de Innovación UC & Microsoft Chile, 2022).

Una de las áreas priorizadas del modelo multidimensional de la Hoja de Ruta es el **Área del Talento y Desarrollo de Competencias para la Ciberseguridad.** Presenta once iniciativas de talento y competencias enfocadas en tres ejes de trabajo. Se priorizaron los proyectos 7,8,10 y 11.

MECANISMOS DE INCENTIVOS A LA INVERSIÓN EN TALENTO	NUEVOS PERFILES, PROGRAMAS Y FORMATOS FLEXIBLES	ASOCIACIONES, COLABORACIÓN PÚBLICO-PRIVADA, CENTROS DE FORMACIÓN Y ACADEMIAS
1 Generar incentivos financieros a privados para levantar infraestructura remota compartida para entrenamiento de talento temprano.	5 Piloto NICE Workforce Framework Cyber CL.	9 Generar una Academia Nacional de Entrenamiento.
2 Asociación con SENCE y sus códigos para incentivos tributarios en formación en ciberseguridad.	6 Programa nacional de capacitación en base a voluntariados de diversas academias, institutos, organismos o empresas.	10 Disponibilidad de centros de desarrollo de talentos a nivel escolar que cuenten con herramientas y recursos.
3 Programa de becas para la especialización basada en financiamiento público.	7 Pilotaje Programa de Magíster en Ciberseguridad BID.	
4 Abrir concursos acotados para licencias gratuitas de softwares para pymes u otras instituciones.	8 Programas in-company de Formación en Ciberseguridad para C-Level y tomadores de decisiones.	11 Asociación público-privada para generación de programas que desarrollen talentos.

Tabla 4. Iniciativas Hoja de ruta de ciberseguridad.
Fuente. Hoja de Ruta de Ciberseguridad.

d. Política Nacional de Ciberseguridad (PNCS) 2023-2028

La Política Nacional de Ciberseguridad incluye diversas iniciativas relacionadas con la formación profesional en ciberseguridad. Esta política plantea la necesidad de desarrollar una cultura de ciberseguridad a nivel nacional, impulsando la educación y capacitación tanto en el sistema educativo formal como a nivel profesional. La PNCS estima que en Chile faltan alrededor de 28.000 especialistas en ciberseguridad para satisfacer las necesidades tanto del sector público como privado, y que, en carreras relacionadas específicamente a la ciberseguridad, solo el 10% son cupos femeninos, cifra que se condice con el 15% de participación de mujeres en los puestos laborales de ciberseguridad que existen en el país. (Ministerio del Interior y Seguridad Pública, 2023).

Entre las acciones destacadas se encuentran:

• **Plan matriz de educación en ciberseguridad:** Se propone generar un plan que abarque desde la educación básica hasta la técnico-profesional y universitaria, con un enfoque en la higiene digital y ciberseguridad.

• **Capacitación continua:** Promover la creación de carreras técnicas en ciberseguridad y la formación continua para empleados en distintos sectores, tanto públicos como privados.

• **Fomento a la investigación:** Se incentiva el desarrollo de investigación aplicada en ciberseguridad, involucrando a la academia, la industria y el sector público, con el fin de generar profesionales capaces de abordar los desafíos futuros en esta área.

• **Alianzas y colaboración público-privada:** Se subraya la importancia de la cooperación entre el sector público y privado para fortalecer las capacidades profesionales en ciberseguridad y coordinar acciones de formación y concienciación.

e. Política Nacional de Inteligencia Artificial de Chile (actualizada en 2024)

Destaca la importancia del desarrollo del talento para abordar los desafíos de la IA, lo cual incluye la formación profesional en ciberseguridad como parte del ecosistema digital seguro.

En el **Eje N°3. Gobernanza y Ética,** se destaca la ciberseguridad y se plantea la necesidad de abordar la IA como un componente relevante en el ámbito de la ciberseguridad y ciberdefensa, promoviendo así sistemas tecnológicos seguros. Las acciones que se proponen, abordan considerar la IA como un componente relevante en el ámbito de la ciberseguridad y ciberdefensa, promoviendo sistemas tecnológicos seguros como: (Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, 2021).

• Incorporar la IA en las estrategias de ciberseguridad y ciberdefensa.

• Fomentar el uso responsable de sistemas de IA para reaccionar a los ataques informáticos en el Estado.

• Fomentar la capacitación en las áreas asociadas a la ciberseguridad e infraestructura crítica.

→V. BENCHMARKING INTERNACIONAL

Foro Nacional de Ciberseguridad (FNC), España. Se creó en julio de 2020, impulsado por el Consejo de Seguridad Nacional, con el objetivo de fomentar la colaboración público-privada, fomentar la cultura de ciberseguridad, ofrecer apoyo a la Industria e I+D+i, promover la formación y el talento y desarrollar la Estrategia Nacional de Ciberseguridad. Centro Criptológico Nacional. (2023).

Figura 4. Estructura de la ciberseguridad en el marco del Sistema de Seguridad Nacional, España.
Fuente: Centro Criptológico Nacional

Este foro actúa como un espacio de encuentro para abordar los retos de ciberseguridad en España, así como la evolución de las amenazas cibernéticas, la necesidad de protección para empresas y ciudadanos, y la capacitación en ciberseguridad. Departamento de Seguridad Nacional. (2023).

En relación con la formación profesional en ciberseguridad, el foro de España posee el grupo de trabajo **"Formación, capacitación y talento"** para promover la capacitación en ciberseguridad adecuada a la demanda del mercado. Ha desarrollado iniciativas centradas en la **creación de un marco de competencias** para programas superiores de formación, fomentando así el desarrollo de habilidades especializadas en este campo. También se han trabajado en propuestas para aumentar la concienciación ciudadana y la **responsabilidad social corporativa** en torno a la ciberseguridad. Además, el foro trabaja en impulsar la industria de la ciberseguridad y promover la I+D+i (Investigación, Desarrollo e Innovación) en colaboración con el sector privado. Foro Nacional de Ciberseguridad. (2023). A continuación, se presentan las acciones definidas por el grupo de trabajo de Formación, capacitación y talento.

Necesidad	Acciones
Promover la capacitación en ciberseguridad adecuada a la demanda del mercado. Detectar, fomentar y retener el talento.	1. Actualizar, o en su caso desarrollar, **marcos de competencias en ciberseguridad**, que respondan a las necesidades del mercado laboral. 2. Identificar las necesidades de capacidades profesionales de ciberseguridad, fomentando la colaboración con las instituciones educativas y formativas impulsando la **formación continua, la formación para el empleo y universitaria, promoviendo sistemas de acreditación y certificación profesional**. 3. Impulsar la inclusión de **perfiles profesionales de ciberseguridad en las relaciones de puestos de trabajo del sector público**. 4. **Detectar, fomentar y retener el talento de ciberseguridad** con especial atención al campo de la investigación. 5. **Impulsar iniciativas y planes de alfabetización digital en ciberseguridad.** 6. Buscar y reconocer la colaboración y participación de medios de comunicación para lograr un **mayor alcance en las campañas dirigidas a ciudadanos y NNA.**

Tabla 5. Acciones del grupo de trabajo Formación, Capacitación y Talento. FNC España.
Fuente: Foro Nacional de Ciberseguridad

→VI. ORGANIZACIONES INTERNACIONALES REFERENTES

a. SANS Institute

Fundado en 1989, el SANS Institute es una de las instituciones líderes a nivel mundial en formación en ciberseguridad. Ofrece una amplia variedad de cursos, certificaciones y programas prácticos en diversas áreas de la seguridad informática. Sus certificaciones GIAC (Global Information Assurance Certification) son ampliamente reconocidas y demandadas en la industria. También es conocido por sus eventos de formación en vivo y sus simulaciones de ciberataques.

b. (ISC)² (International Information System Security Certification Consortium)

(ISC)² es una organización mundial sin fines de lucro conocida por ofrecer la certificación CISSP (Certified Information Systems Security Professional), una de las más reconocidas en el campo de la ciberseguridad. Además, (ISC)² proporciona programas de formación y certificación para otras áreas de la seguridad de la información, con el objetivo de mejorar las competencias y conocimientos de los profesionales de ciberseguridad.

c. EC-Council (International Council of E-Commerce Consultants)

Es una organización líder a nivel mundial en educación, certificación y capacitación en ciberseguridad, con sede en Albuquerque, Nuevo México, EE.UU. Fundada en 2001, EC-Council es conocida por su enfoque en la seguridad ofensiva y defensiva, ofreciendo programas de certificación de alta demanda como:

- **Certified Ethical Hacker (CEH):** Su certificación más famosa, enfocada en enseñar a los profesionales de seguridad las mismas técnicas que usan los hackers malintencionados para detectar y proteger vulnerabilidades. Es una certificación ampliamente respetada y solicitada en el mercado laboral.

- **Certified Network Defender (CND):** Un curso orientado a la seguridad de redes, que enseña a los profesionales cómo proteger, detectar y responder a incidentes de seguridad en las redes de una organización.

- **Computer Hacking Forensic Investigator (CHFI):** Esta certificación está diseñada para profesionales interesados en la investigación forense digital, enseñándoles técnicas y herramientas para identificar, rastrear y documentar actividades cibercriminales.

EC-Council ha certificado a miles de profesionales en más de 140 países, ayudando a cubrir la brecha de habilidades en ciberseguridad mediante programas de certificación reconocidos por organizaciones gubernamentales, empresas y organismos de defensa en todo el mundo. También organiza eventos y conferencias globales, como la Global CyberLympics y Hacker Halted, para fomentar el aprendizaje continuo y la colaboración en la industria de la ciberseguridad.

d. ISACA (Information Systems Audit and Control Association)

Es una organización global sin fines de lucro fundada en 1969, dedicada a la auditoría, gobernanza, seguridad de la información, gestión de riesgos y ciberseguridad. ISACA es ampliamente reconocida por sus certificaciones, recursos y estándares de referencia en el ámbito de las tecnologías de la información y la ciberseguridad, y desempeña un papel importante en la formación y certificación de profesionales de TI.

ISACA ofrece varias certificaciones prestigiosas, que son valoradas en los sectores de auditoría, seguridad de la información y ciberseguridad:

- **Certified Information Systems Auditor (CISA):** Esta certificación es uno de los estándares más reconocidos en auditoría de sistemas de información. Está dirigida a profesionales que gestionan y aseguran los sistemas informáticos y están involucrados en la gobernanza y control de TI.

- **Certified Information Security Manager (CISM):** Enfocada en la gestión de la seguridad de la información, CISM es ideal para quienes supervisan y gestionan los programas de seguridad dentro de las organizaciones.

- **Certified in Risk and Information Systems Control (CRISC):** Esta certificación se centra en la gestión de riesgos y control de sistemas de información. Está dirigida a aquellos que identifican, evalúan y gestionan riesgos en TI.

- **Certified in the Governance of Enterprise IT (CGEIT):** Esta certificación está orientada a la gobernanza de TI empresarial. CGEIT está dirigida a profesionales que lideran la implementación de marcos de TI en sus organizaciones para garantizar el cumplimiento de objetivos empresariales.

- **Cybersecurity Nexus (CSX):** La serie de certificaciones CSX es relativamente nueva y fue creada para responder a la demanda de profesionales capacitados en ciberseguridad. Ofrece formación práctica en ciberseguridad y certificaciones en diferentes niveles de competencia.

Estándares y Buenas Prácticas: ISACA desarrolla y mantiene marcos como COBIT (Control Objectives for Information and Related Technologies), un estándar ampliamente utilizado para la gobernanza y gestión de TI que ayuda a las empresas a maximizar el valor de sus recursos de TI.

Educación Continua: ISACA organiza eventos, conferencias, talleres y webinars, además de ofrecer programas de educación continua para sus miembros y para la comunidad global de TI.

Red Profesional: Con más de 150,000 miembros en todo el mundo, ISACA ofrece una red global de profesionales de TI que permite la colaboración, el intercambio de conocimientos y la construcción de una comunidad en constante evolución en temas de ciberseguridad, auditoría, gobernanza y gestión de riesgos.

ISACA se ha consolidado como un referente en la industria, estableciendo estándares y certificaciones de calidad que han ayudado a construir una base sólida de profesionales de TI en roles críticos para la seguridad y el desarrollo tecnológico en organizaciones de todo el mundo.

→ VII. PRINCIPALES HALLAZGOS DEL BENCHMARKING NACIONAL E INTERNACIONAL EN FORMACIÓN Y DESARROLLO PROFESIONAL EN CIBERSEGURIDAD.

Este análisis revela la importancia de crear políticas integrales que incluyan a diferentes sectores y promuevan tanto la educación como la capacitación profesional en ciberseguridad, preparando a la sociedad para enfrentar los desafíos cibernéticos emergentes. El benchmarking nacional e internacional sobre formación y desarrollo profesional en ciberseguridad destaca que, tanto en Chile como España, hay un enfoque creciente en la creación de programas de formación especializados para abordar las brechas de talento y fortalecer las capacidades en ciberseguridad.

1. Enfoque nacional e internacional en la formación técnica y profesional. Chile y España, a través de políticas como la Estrategia de Transformación Digital y la Política Nacional de Ciberseguridad, promueven la creación de programas de formación, certificación y especialización en ciberseguridad.

2. Colaboración público-privada. Ambos países reconocen la importancia de involucrar al sector privado, la academia y el sector público para desarrollar capacidades, con iniciativas de formación continua, certificación y colaboración en investigación e innovación.

3. Fomento de la inclusión y equidad de género. Se visibiliza la necesidad de reducir la brecha de género en el campo de la ciberseguridad, con iniciativas para atraer a más mujeres a programas de ciberseguridad tanto en Chile como en España.

4. Necesidad de actualizar marcos de competencia. La creación de marcos de competencias alineados con estándares internacionales como el CMM de Oxford y la promoción de la certificación profesional son esenciales para asegurar que la fuerza laboral esté preparada para enfrentar las amenazas cibernéticas actuales y futuras.

A continuación, se presenta un resumen con las iniciativas apalancadas desde las distintas políticas y estrategias nacionales e internacionales, que han plasmado desafíos para el desarrollo de las capacidades profesionales en ciberseguridad. Esto resume los esfuerzos en formación profesional en ciberseguridad, mostrando cómo cada iniciativa se enfoca en desarrollar talento y capacidades en este campo, promoviendo la colaboración entre los sectores público y privado, así como el fomento de la inclusión de mujeres en la industria.

Iniciativa	Acciones Propuestas
Estrategia de Transformación Digital, Chile Digital 2035	• Creación del Instituto Nacional de Ciberseguridad y del Centro de Capacidades de Ciberseguridad de Iberoamérica al 2023. • Establecer un plan nacional de reconversión de la fuerza laboral para trabajos que desaparecerán. • Mejora de la oferta educativa en ciberseguridad con programas de acreditación. • Formación de 10.000 profesionales certificados en Ciberseguridad al 2035, donde al menos el 30% de ellos sean mujeres. • Alcanzar el 2035 una "Madurez en Ciberseguridad" cercana al Estado 5 o "Dinámico".
Construyendo la Ciberseguridad.	• Generación de Diplomas y Certificaciones de Competencia. • Capacitación de empresas y organismos estatales. • Realizar un catastro y diagnóstico en distintas Instituciones del nivel de ciberseguridad. • Generar la "Plataforma nacional de Ciber formación y ciber empleos– orientado a Ciberseguridad. • Realizar un estudio para estimar demandas y público objetivo. • Generar ferias laborales con foco en reconversión laboral. • Creación del Instituto Nacional de Ciberseguridad (INCIBER) • Crear un equivalente de la Estonian Defence League's Cyber Unit de Estonia.
Hoja de Ruta de Ciberseguridad (Microsoft y UC)	• Generar incentivos financieros para levantar infraestructura remota para entrenamiento de talento temprano. • Asociación con SENCE y sus códigos para incentivos tributarios en formación en ciberseguridad. • Programa de becas de especialización con financiamiento público. • Abrir cursos acotados para licencias gratuitas de software para pymes y otras instituciones. • Piloto NICE. • Programa nacional de capacitación en base de voluntariado. • Pilotaje Programa de Magister en Ciberseguridad BID. • Programas in-company de formación en ciberseguridad para C-Level y tomadores de decisiones. • Generar una academia nacional de entrenamiento. • Disponibilidad de centros de desarrollo de talentos.

Política Nacional de Ciberseguridad (PNCS) 2023-2028	• Plan de educación desde la educación básica hasta profesional en ciberseguridad. • Capacitación continua en ciberseguridad para empleados públicos y privados. • Promoción de la investigación aplicada en ciberseguridad. • Potenciar alianzas y colaboración público-privada para fortalecer capacidades profesionales en ciberseguridad y coordinar acciones de formación y concienciación.
Política Nacional de Inteligencia Artificial (2024)	• Incorporar la IA en estrategias de ciberseguridad y ciberdefensa. • Fomentar el uso responsable de sistemas de IA frente a ataques informáticos. • Impulsar la capacitación en infraestructura crítica y ciberseguridad.
Foro Nacional de Ciberseguridad de España	• Promover la capacitación en ciberseguridad a la demanda del mercado. • Detectar, fomentar y retener el talento en ciberseguridad. • Crear marcos de competencias para programas superiores de formación. • Fomentar la capacitación continua y certificación profesional. • Aumentar la colaboración entre el sector público y privado. • Incluir la alfabetización digital en ciberseguridad. • Impulsar la inclusión de perfiles profesionales de ciberseguridad en el sector público.

→ VIII. ÉTICA

El grupo de trabajo profundiza en la ética como una disciplina relevante que debe ser desarrollada en los profesionales insertos en la ciberseguridad. La **ética** se define como la disciplina filosófica que estudia los principios que determinan lo que es **correcto** o **incorrecto** en el comportamiento humano, buscando guiar las acciones hacia lo **bueno** y lo **justo** en la convivencia social.

En otros términos, la ética se refiere al **conjunto de principios** que determinan cómo **debe comportarse una persona** en su vida diaria, en relación con otras personas, relaciones laborales y cómo se debe enfrentar la resolución de dilemas morales. Por consiguiente, la ética juega un papel fundamental, ya que establece los estándares de conducta que los profesionales deben seguir para garantizar el bienestar de la sociedad, el respeto a las leyes y normas, y la confianza pública.

Para la ética se destacan conceptos claves:

• **Responsabilidad:** Ser consciente de las consecuencias de las propias acciones.

• **Justicia:** Tratar a los demás con equidad, imparcialidad y respeto.

• **Honestidad:** Actuar con transparencia y sinceridad en las relaciones interpersonales.

• **Integridad:** Mantenerse fiel a los principios personales y profesionales, incluso cuando no hay observadores.

Estos conceptos no solo describen características de comportamiento deseables, sino que se convierten en la base de principios éticos fundamentales que guían la práctica profesional.

a. Principios Éticos Fundamentales.

Estos principios éticos son aplicables no solo en Chile, sino a nivel global, y son fundamentales para guiar el trabajo de un profesional en informática:

• Confianza y Responsabilidad. Los profesionales deben ser dignos de confianza, garantizando la seguridad y privacidad de los usuarios, y asegurando que sus desarrollos sean confiables y no vulnerables a ciberataques o mal uso.

• Integridad Profesional. Los profesionales deben actuar con honestidad en todo momento. Esto incluye ser transparentes sobre las capacidades y limitaciones de sus sistemas, y no comprometer sus estándares éticos ni la seguridad de los usuarios por intereses comerciales o personales.

• Impacto Social y Ambiental. Los profesionales deben estar comprometidos con el bienestar social y el impacto positivo de la tecnología. Deben evitar el desarrollo de sistemas que puedan tener efectos negativos en la sociedad, como algoritmos sesgados o software que amplifique desigualdades sociales.

• Desarrollo Sostenible. Los profesionales deben tener en cuenta el desarrollo sostenible en el diseño de sistemas, garantizando que sus tecnologías sean accesibles, respetuosas con el medio ambiente y que contribuyan a un futuro digital inclusivo y sostenible.

b. Principios Éticos Específicos para profesionales de la Informática

Estos principios éticos se enfocan en áreas específicas como la **seguridad cibernética, la protección de datos y el uso responsable de la tecnología.**

Desarrollo Responsable de Tecnologías.

• **Calidad del software:** Deben asegurarse de que sus productos sean funcionales, robustos y seguros. Esto incluye la realización de pruebas exhaustivas para detectar vulnerabilidades que puedan poner en riesgo a los usuarios o comprometer la seguridad de los sistemas.

• **Transparencia en algoritmos y IA:** Deben ser transparentes en el uso de algoritmos y sistemas de inteligencia artificial (IA), especialmente si estos afectan decisiones importantes como la contratación de personal, la evaluación crediticia o el diagnóstico médico o comprometen la seguridad pública.

Seguridad y Protección de Datos

• **Privacidad de los usuarios:** Deben garantizar que la información personal de los usuarios esté protegida mediante medidas adecuadas de seguridad. Además, deben cumplir con las regulaciones locales y/o internacionales sobre privacidad.

• **Ciberseguridad:** Los sistemas que diseñan deben ser resistentes a ciberataques, garantizando la integridad de los datos y la protección de las infraestructuras críticas. Esto implica gestionar, diseñar y desarrollar sistemas que sigan los estándares más altos de seguridad informática.

Uso Responsable de la Tecnología

• **Impacto social de la tecnología:** Un profesional del área debe ser consciente de los efectos que sus desarrollos tienen sobre la sociedad, como el potencial uso indebido de tecnologías o la creación de sistemas que puedan discriminar a ciertos grupos de personas.

• **Brecha digital e inclusión:** Todo desarrollo de tecnologías deben ser accesibles para todos, evitando contribuir a la brecha digital y promoviendo la inclusión digital de grupos vulnerables.

Además de los principios éticos generales, los profesionales del área deben procurar que sus actividades cumplan con las directrices de leyes y normas específicas que abordan temas clave como la **protección de datos, la seguridad cibernética y el uso de tecnologías emergentes:**

a) Ley N° 19.496: Ley sobre Protección de la Vida Privada (Protección de Datos Personales)
b) Ley N° 21.153: Ley sobre Delitos Informáticos
c) Ley N° 20.009: Ley de Firma Electrónica
d) Ley N° 20.585: Ley sobre el Uso de la Tecnología para la Prevención de Delitos

Las actividades de los profesionales del área informática, en Chile está regida por principios éticos y normativas que se alinean con las regulaciones generales para todos los técnicos e ingenieros, pero también incluyen aspectos específicos relacionados con la **seguridad cibernética, la protección de datos, y el uso responsable de la tecnología.** Estos principios éticos y las leyes relevantes (como la Ley de Protección de Datos y la Ley de Delitos Informáticos) proporcionan un marco que asegura que los ingenieros informáticos desarrollen soluciones tecnológicas que respeten los derechos de los usuarios, promuevan la inclusión digital y tengan un impacto social positivo, todo mientras se mantienen a la vanguardia de la innovación y el cumplimiento normativo.

→ IX. HABILIDADES BLANDAS O TRANSVERSALES

El desarrollo de habilidades blandas o transversales en los profesionales de ciberseguridad es un aspecto crucial para complementar sus capacidades técnicas y permitir un desempeño integral en un entorno altamente dinámico y colaborativo. Estas habilidades permiten a los profesionales interactuar efectivamente con equipos multidisciplinarios, educar y sensibilizar sobre la importancia de la ciberseguridad, y liderar iniciativas dentro de las organizaciones para construir una cultura de seguridad cibernética sólida.

El marco NICE (Workforce Framework for Cybersecurity) identifica habilidades clave como comunicación efectiva, liderazgo, colaboración, pensamiento crítico y gestión de conflictos, que son esenciales para los profesionales de ciberseguridad. Sin embargo, la incorporación de estas habilidades en los programas de formación sigue siendo un desafío, debido a la predominancia de enfoques exclusivamente técnicos en la educación actual.

Con la incorporación del desarrollo de estas habilidades en las distintas etapas de formación de un profesional, se generará un profesional que:

- Asuma la responsabilidad de sus tareas y de lo que significa tener en sus manos información privilegiada, entregue resultados de alta calidad y corrija errores cuando sea necesario.

- Responda rápidamente, con flexibilidad y resiliencia a las contingencias que el entorno de ciberseguridad requiere.

- Trabaje en equipo, debido a la transversalidad de la ciberseguridad, es necesario que trabaje en conjunto con las distintas áreas de la empresa (privada o pública) y que logre segurizar ambientes de trabajo.

- Desarrolle de buena forma políticas, informes, planes, etc, escuchando activamente y transmitiendo ideas claramente.

- Maneje conflictos de manera constructiva y lograr la cohesión del equipo como asimismo el compromiso de la empresa en su totalidad.

- Analice datos y sistemas para poder tomar decisiones informadas.

- Adapte a las nuevas tecnologías y amenazas.

- Sea capaz de influenciar a su entorno laboral para la buena implementación y ejecución de las políticas de ciberseguridad, contribuyendo en el diseño de planes estratégicos y en la toma de decisiones tecnológicas.

- Sea proactivo, independiente y creativo en la solución de problemas.

- Trabaje con ética y fomentar la confianza en el entorno de trabajo.

- Se mantenga en aprendizaje continuo

• Sea capaz de practicar la empatía, sensibilidad cultural y regulación emocional para un buen clima laboral.

• Aborde desafíos complejos usando habilidades como la flexibilidad y colaboración para poder llevar a cabo una buena resolución de problemas.

• Finalmente, debe ser capaz de planificar a largo plazo, con visión de futuro, para minimizar riesgos y aprovechar oportunidades.

Para desarrollar estas habilidades de forma efectiva, Pacheco (n.d), indica que se puede incorporar en la enseñanza dinámicas basadas en juegos prácticos, colocando al alumno en situaciones simuladas y controladas donde se trabaje las distintas resoluciones que puede tener un caso de uso en particular; o también dinámicas basadas en juegos, con competiciones del tipo Captura de bandera (CTF).

La ciberseguridad, aunque comúnmente se asocia al ámbito de la informática, tiene un impacto transversal que abarca diversas áreas laborales, como la técnica, social, financiera y legal. Por ello, es esencial que la formación de profesionales en ciberseguridad, especialmente en modalidades de educación continua, incorpore la perspectiva y aportes de expertos de distintos campos. De este modo, se enriquece tanto el aprendizaje como la práctica y la evolución del estado del arte en ciberseguridad, favoreciendo un enfoque multidisciplinario que potencia su desarrollo.

→ X. PRINCIPALES DESAFÍOS Y PROPUESTAS

El desarrollo y fortalecimiento de capacidades en ciberseguridad se presenta como un desafío estratégico de cara a las crecientes demandas del entorno digital. Los avances tecnológicos y la complejidad de las amenazas cibernéticas exigen una respuesta integrada que abarque la formación profesional, la innovación en metodologías educativas, y la colaboración entre sectores público, privado y académico.

Este capítulo analiza los principales desafíos identificados en el Foro Nacional de Ciberseguridad y propone acciones concretas, basadas en un enfoque colaborativo, que permitan cerrar brechas críticas y fomentar un ecosistema robusto en ciberseguridad. La meta es alcanzar niveles de madurez que conviertan a Chile en un referente regional en formación y capacidades cibernéticas, alineado con los estándares internacionales y las necesidades locales.

Desafíos	Acciones	Impacto Esperado
Escasez de profesionales en ciberseguridad en Chile.	Crear programas de formación profesional y certificación en ciberseguridad, además de becas y planes de reconversión laboral para aumentar la oferta de especialistas, con financiamiento público. Realizar estudios para estimar demandas reales de perfiles, habilidades y público objetivo. Permite focalizar los planes de formación. Generar plataforma nacional de Ciber formación y ciber empleos, orientado a Ciberseguridad. Nivelar conocimientos en competencias básicas como bases de datos, programación y redes, para que estudiantes que entran a estudiar ciberseguridad, enfrenten de mejor forma los procesos de formación, reskilling y upskilling.	Aumento en la oferta de especialistas, mejora en la empleabilidad y fortalecimiento del sector.

Disminuir la brecha de género en el campo de la ciberseguridad (baja participación femenina).	Fomentar la inclusión de mujeres en carreras de ciberseguridad y establecer cuotas de participación femenina en programas educativos y certificaciones. En todas las iniciativas propuestas revisar la incorporación femenina y generar mecanismos para aumentar su participación, como becas, difusión focalizada, entre otros.	Mayor inclusión, diversidad y equidad en la fuerza laboral de ciberseguridad.
Actualizar las competencias profesionales en ciberseguridad.	Desarrollar marcos de competencias nacionales alineados con estándares internacionales como (NICE, Marco europeo) que respondan a las necesidades del mercado laboral, que permita ofrecer programas de formación continua y certificación profesional asegurando la movilidad y reconocimiento profesional. Generar y potenciar la colaboración internacional. Crear alianzas con organismos internacionales (por ejemplo, ENISA o INCIBE) para compartir buenas prácticas y acceder a programas de capacitación avanzada.	Actualizar competencias profesionales alineadas con estándares internacionales, fortalecerá la empleabilidad, innovación, movilidad laboral, colaboración global y posicionamiento estratégico de Chile.
Baja madurez y medición de la ciberseguridad del sector público y privado.	Implementar diagnósticos de madurez en ciberseguridad en instituciones y fomentar la mejora continua mediante la capacitación. Priorizar el sector público.	Fortalecer la resiliencia institucional, optimizando recursos y promoviendo estándares nacionales.
Falta de cooperación público-privada en ciberseguridad.	Establecer alianzas estratégicas entre el sector público, privado y académico para la formación y el desarrollo de capacidades en ciberseguridad. Promover programas de formación específicos por sector. Algunos organismos involucrados: SENCE, ChileValora, Asociaciones Gremiales, Vertebral, Consejo de Rectores, Corfo, CPC.	Fortalecimiento del ecosistema de formación en ciberseguridad, optimización de recursos y mayor cohesión entre sectores clave.

Integración de inteligencia artificial en la ciberseguridad.	Incorporar IA en estrategias de ciberseguridad y ciberdefensa, además de fomentar la capacitación en el uso de IA para la detección y respuesta a amenazas cibernéticas.	Innovación en herramientas de detección y respuesta, adaptabilidad frente a nuevas amenazas.
Escasez de infraestructuras para la capacitación y entrenamiento en ciberseguridad.	Crear centros de entrenamiento especializados con infraestructura avanzada para el desarrollo de ejercicios presenciales y remotos. (Se menciona Inciber y la Agencia Nacional de Ciberseguridad). Organizar ejercicios nacionales e internacionales. Generar un mecanismo de observación permanente para identificar nuevas tecnologías, actualizaciones, convenios y otros.	Mejorar la preparación práctica y actualización constante frente a nuevas amenazas.
Falta de formación de especialistas en habilidades docentes para transmitir conocimiento.	Desarrollar habilidades docentes entre especialistas en ciberseguridad para mejorar la transferencia de conocimientos en programas educativos y formativos. Programas Train the trainers (programa de desarrollo y fortalecimiento de competencias de relatoría y facilitación de aprendizajes al interior de una organización).	Mejora en la calidad y capacidad de transferencia de conocimientos en el ámbito académico.
Fomentar la ética en ciberseguridad.	Incorporar en las instancias de formación enfoques éticos basados en principios como integridad, responsabilidad, justicia y transparencia. Simular escenarios donde los profesionales deban tomar decisiones basadas en estos principios.	Fortalecimiento de la confianza pública y privada en los profesionales de ciberseguridad, garantizando prácticas responsables y transparentes.
Desarrollar habilidades blandas o transversales que permitan un desempeño integral desde la colaboración, interrelaciones, transferencia de conocimientos y convencer a la organización de la importancia de la ciberseguridad.	Incorporar en los programas de formación habilidades como comunicación efectiva, liderazgo, gestión de conflictos, negociación y presentación de ideas.	Fortalecer los mecanismos de comunicación y la importancia de la ciberseguridad de manera clara y persuasiva, logrando un mayor compromiso de las organizaciones para implementar medidas de seguridad.

→ XII. PROPUESTA PRÓXIMOS PASOS

A continuación, se proponen algunas actividades para el equipo que continuará participando del Foro Nacional de Ciberseguridad.

• **Fortalecer los grupos de trabajo actuales.** Incorporar nuevos participantes de sectores clave (industria, academia, organizaciones civiles) para enriquecer la discusión.

• **Fomentar la integración de perspectivas interdisciplinarias.** Incluir expertos en áreas complementarias (educación, ética, derecho, psicología) para abordar la ciberseguridad desde una visión integral.

• **Hacer seguimiento al estado de avance de las iniciativas ya existentes.** Entrevistar a los responsables de las iniciativas levantadas en el benchmarking, identificar los estados de avances, resultados e impactos de las acciones implementadas.

• **Apoyar iniciativas en desarrollo.** Colaborar con iniciativas en desarrollo que se vean fortalecidas con la experiencia de quienes se encuentran participando del foro. Levantamiento de perfiles, marcos de cualificaciones, programas de formación, certificaciones, entre otros.

• **Desarrollar un plan operativo anual.** Definir metas trimestrales para avanzar en las acciones 2025.

• Continuar coordinando con los otros grupos de trabajo del foro.

→ D3.4 Propuestas para Fortalecer la Madurez en Investigación e Innovación en Ciberseguridad en Chile.

Es un honor dirigirnos a ustedes en representación del Foro de Ciberseguridad, Dimensión D3.4, una instancia que reúne a expertos de diversos sectores públicos y privados, así como de la Academia, con el objetivo de promover la Investigación e Innovación para el fortalecimiento de la ciberseguridad en nuestro país. En este contexto, les presentamos algunos elementos destacables en el camino hacia la madurez en Investigación e Innovación en Ciberseguridad en Chile, de los cuales es posible extraer un conjunto de recomendaciones clave para avanzar hacia el fortalecimiento de nuestra soberanía digital y tecnológica y el mejoramiento de capacidades para I+D en estas áreas.

Este documento primero realiza una autoevaluación del factor D3.4 del **Modelo de Madurez de Capacidades en Ciberseguridad (CMM)** desarrollado por el **Centro Global de Capacidades en Ciberseguridad de la Universidad de Oxford,** el cual deberá ser contrastado con la evaluación que se realice este año en la dimensión 3.4 del modelo de Oxford, postulando - como situación actual - que el País se encuentra en **un nivel Formativo** de Capacidades de I+D en ciberseguridad. Aunque Chile ha dado pasos importantes en la regulación y concienciación sobre ciberseguridad, es claro también que la investigación científica y su traspaso a la sociedad, así como el estímulo activo de las innovaciones que de ella se derivan, juegan un rol importantísimo en el camino hacia la madurez de nuestra sociedad en Seguridad de la Información, y por lo tanto podemos considerar que en este camino, la investigación e innovación se encuentran aún en sus primeras fases. Es necesario y pertinente, por lo tanto, mantener, propiciar e incrementar la inversión en I+D, establecer colaboraciones estratégicas tanto a nivel nacional como internacional, desarrollar el talento especializado y adoptar métricas claras para medir el progreso en estos dominios. Con estos elementos, Chile podrá consolidarse con orgullo propio, como un país capaz de innovar en ciberseguridad y enfrentar de manera eficaz los riesgos emergentes del ciberespacio.

Segundo, este documento propone como **situación futura a 4 años, alcanzar el nivel "Estratégico".** Y tercero, **propone un conjunto de acciones a incluir en el Plan de Acción de la Política Nacional de Ciberseguridad que son prioritarias para alcanzar el nivel esperado o situación futura a 4 años desde su ejecución.**

Estamos convencidos de que la adopción de estas propuestas, orientadas a fortalecer la investigación y la innovación en ciberseguridad, contribuirá significativamente a consolidar la resiliencia digital de nuestro país, mejorar su competitividad global y proteger a nuestros ciudadanos frente a las amenazas emergentes. Contamos con su apoyo para incluir estas recomendaciones en la agenda legislativa y avanzar hacia un futuro más seguro para Chile. Quedamos a su disposición para discutir estas propuestas en mayor detalle y esperamos con interés su apoyo para implementar estas necesarias mejoras.

Atentamente,

Equipo de Redacción.

→ Resumen ejecutivo

El Foro Nacional de Ciberseguridad se propuso realizar una evaluación del nivel de madurez de Chile en función del modelo de Oxford (CMM). Esto con el fin de establecer una evaluación del estado del arte en estas materias e identificar el camino a seguir para elevar el nivel de madurez identificado. Éste proceso ha permitido identificar las brechas y establecer planes de acción para la mejora continua utilizando el modelo de Oxford. El presente documento, contiene los resultados del trabajo realizado y las recomendaciones necesarias para mitigar los actuales riesgos en relación al Factor D3.4: Investigación e Innovación en Ciberseguridad", perteneciente a la dimensión 3 del modelo (Educación, Capacitación y Habilidades en Ciberseguridad). Cabe considerar que es la primera vez que esta dimensión se mide en el país.

El objetivo del proceso estuvo centrado en entender el modelo de Oxford, realizar un levantamiento de la situación actual y finalmente establecer recomendaciones priorizadas. Estos resultados se han comparado con el estándar antes mencionado, con el fin de poder determinar áreas de mejora que puedan ser desarrolladas en el tiempo. La metodología utilizada para el desarrollo de este diagnóstico ha consistido en:

- **Entender el modelo de Oxford (CMM) con el fin de establecer los requisitos necesarios para cumplir con algún nivel de madurez;**

- **Entender la situación actual del País, lo que permite entre otros aspectos; identificar y conocer iniciativas y proyectos de investigación avanzada en ciberseguridad, identificar y conocer los objetivos de Chile en éstas materias y las iniciativas en curso;**

- **Realizar una identificación de regulaciones, documentos e iniciativas claves que promuevan o declaren aspectos ligados a la investigación avanzada en ciberseguridad, dentro de estos se destaca en el análisis la Política Nacional de Ciberseguridad (2023- 2028), el estudio Construyendo la Ciberseguridad en Chile (2022) y el Informe I+D en Ciberseguridad (2024), entre otros;**

- **Realizar una evaluación en función de los criterios de madurez establecidos en el modelo;**

- **Realizar una identificación del riesgo de no madurar en estos ámbitos;**

- **Realizar recomendaciones y planes de acción para asegurar un ecosistema sostenible para la investigación avanzada en ciberseguridad, y en específico, recomendaciones para el regulador;**

- **Entregar los resultados del proceso en un informe final.**

Para cumplir con los objetivos planteados, se establecieron comunicaciones directamente a través de la plataforma del foro y a través de otros mecanismos tecnológicos. Se realizaron también diversas entrevistas, con personas claves del ecosistema de ciberseguridad del país, como lo es el actual Coordinador Nacional de Ciberseguridad y el Encargado del CSIRT de Gobierno.

Como se indicó anteriormente en términos de madurez en materia de investigación e innovación en ciberseguridad, Chile presenta un nivel de madurez “Formativo” de Capacidades de I+D. Ubicando al país con un nivel de madurez bajo en éste tipo de temas. Aunque Chile ha dado pasos importantes en materia de regulación, alianzas y concienciación sobre ciberseguridad, aún falta formalizar una estructura y/o institucionalidad robusta que haga sostenible la investigación avanzada en Chile.

Se ha identificado que las áreas de enfoque de investigaciones son diversas, lo que resalta la amplitud de la ciberseguridad como disciplina. Cada uno de estos temas aborda aspectos críticos de la ciberseguridad, desde la protección de infraestructura crítica hasta la educación, prevención y gestión de riesgos. El enfoque multifacético de estas investigaciones refleja la complejidad de las amenazas actuales y futuras. Uno de los principales problemas que comparten los investigadores, es la falta de financiamiento adecuado. Se destaca que las barreras para acceder a fondos estatales o a apoyos institucionales dificultan el desarrollo a largo plazo de iniciativas en I+D, especialmente en áreas tan complejas y cambiantes como la ciberseguridad. A pesar de los obstáculos financieros, las instituciones y sus investigadores están desarrollando soluciones innovadoras en sus respectivas áreas. Cada uno, espera poder contribuir de forma significativa a nivel local.

En cuanto a las recomendaciones para fortalecer el ecosistema de I+D y elevar el nivel de madurez al estado siguiente “Establecido”, se deberá fomentar la colaboración entre los actores clave, y crear un marco regulatorio que favorezca una estructura sostenible y de mejora continua en estos temas. Las principales recomendaciones de éste documento se centran en:

1. Creación de un centro de referencia nacional: Se propone la creación de un Centro Nacional de Investigación en Ciberseguridad que coordine los esfuerzos de I+D, fomente la colaboración y atraiga inversión extranjera.

2. Fomento de la colaboración público-privada: Se recomienda establecer un ecosistema colaborativo entre academia, industria y gobierno a través de incentivos fiscales y subsidios para proyectos conjuntos.

3. Desarrollo de infraestructura compartida: Se propone la creación de un Laboratorio Nacional Distribuido para I+D en Ciberseguridad que permita a las instituciones y empresas probar y desarrollar nuevas tecnologías.

4. Marco regulatorio claro: Se requiere un marco legal que regule la investigación y el desarrollo en ciberseguridad, garantizando una innovación responsable y segura.

5. Desarrollo de capital humano avanzado: Se deben aumentar los programas de formación en ciberseguridad y ofrecer incentivos para que las empresas ofrezcan prácticas profesionales.

6. Incentivos para la innovación y el emprendimiento: Se deben establecer beneficios fiscales y apoyo financiero para las startups que trabajen en ciberseguridad.

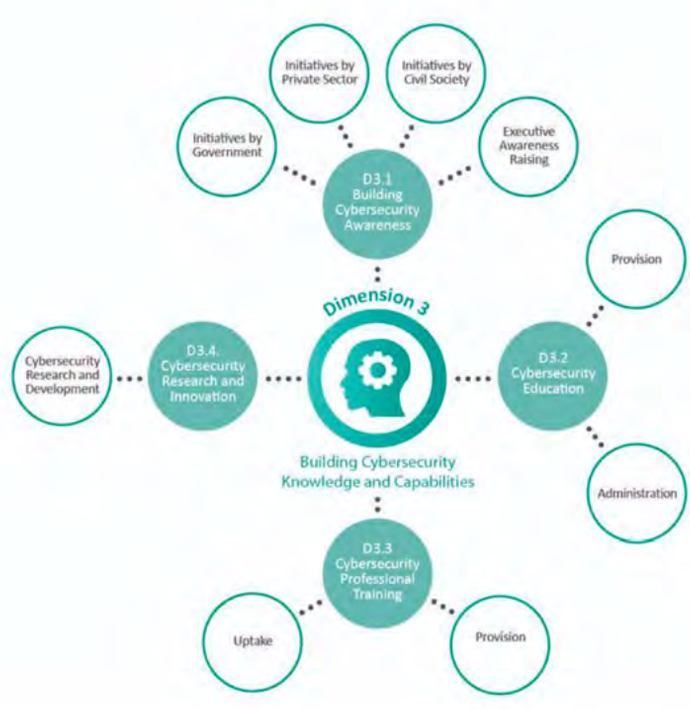
7. Actualización periódica de la estrategia nacional: Se debe revisar y actualizar la Estrategia Nacional de Ciberseguridad para adaptarla a las nuevas amenazas y tecnologías emergentes.

En resumen, el fortalecimiento de la investigación e innovación en ciberseguridad en Chile requiere de una acción coordinada entre el gobierno, la academia y el sector privado. La implementación de estas recomendaciones permitirá a Chile posicionarse como un referente regional en ciberseguridad y contribuir al desarrollo de soluciones innovadoras para enfrentar los desafíos actuales y futuros en este ámbito. Los detalles de estos análisis y resultados se presentan en las siguientes páginas de éste documento.

Situación base del País en investigación avanzada en Ciberseguridad

→Modelo de Oxford

En las evaluaciones aplicadas a Chile, no se ha considerado el Factor D3.4: Investigación e Innovación en Ciberseguridad, perteneciente a la dimensión 3 del modelo (Educación, Capacitación y Habilidades en Ciberseguridad), ya que este factor fue incorporado en la versión publicada en 2021.



Tal como se puede apreciar en la siguiente Tabla, un País puede tener un nivel de madurez "inicial", "formativo", "establecido", "estratégico" o "dinámico" en materia de Investigación e Innovación en Ciberseguridad.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Research and Development	There are limited or no cybersecurity research and development (R&D) activities occurring in the country. There is no access to R&D activities in cybersecurity from other countries.	Some integration of cybersecurity R&D activities occurs within the country, or with a partner country that understands how cyberactivity R&D applies to the local context of the country. The country may participate in relevant regional/ international cybersecurity-related research collaboration networks. Cybersecurity R&D performance metrics are limited in scope, or *ad hoc*.	Cybersecurity R&D activities have been established and are indicated in the national cybersecurity strategy. R&D strategy may be in development. The resources and processes required to deliver the actions of cybersecurity R&D activities have been identified and are in place. Funding is adequate to deliver these actions. There is active regional/ international collaboration with leading practice and developments. The country is actively participating and contributing to regional/ international cybersecurity-related research collaboration networks. Metrics for measuring R&D performance are in place and allow progress to be measured and to improve the cybersecurity R&D capability of the country.	The country is actively building communities of interest around R&D priorities in cybersecurity. R&D strategy is in place and fully implemented. The country makes a major contribution to cybersecurity R&D and is actively involved in building innovation capacity through international R&D consortia and investment. Emerging cybersecurity risks are regularly assessed and used to update the national cybersecurity strategy and the development of future programmes of the R&D strategy. Synergy between academic institutions and industry supports R&D activities and is used to design cyber curricula that cover industry needs.	The country is a leading actor in cybersecurity research and innovation and is shaping international debates on the development of R&D strategic plans. The country is forward looking, seeing emerging issues (around new technology or new types of threat), and uses R&D to prepare a future threat environment. The country is contributing to international best practices in cybersecurity R&D.

Factor - D3.4: *Cybersecurity Research and Innovation*

Tal como explicita el capítulo V del Libro **"Construyendo la Ciberseguridad en Chile"** Acorde a la submesa de investigación avanzada de ciberseguridad, el **País presentaba en 2022** un nivel formativo en el factor 3.4 de Investigación e Innovación en Ciberseguridad, situación que - al momento de escribir este reporte, no había sido efectivamente medida.

A pesar de haber contado con una Política Nacional de Ciberseguridad (2017-2022) y una actual en el periodo 2023-2028, junto con una creciente conciencia sobre la ciberseguridad, aún se evidencian brechas que permiten conjeturar que es poco probable que el nivel de madurez en este factor se mueva desde la línea de "formativo" a "establecido" (siguiente nivel), dado los siguientes antecedentes:

• Las actividades de I+D en ciberseguridad no han sido establecidas de manera explícita. Aún cuando en la Política Nacional de Ciberseguridad (PNC 2023-2028) se indica la necesidad de generar y financiar investigación y desarrollo (I+D) en ciberseguridad, sobre todo en aquellas áreas que, sirviendo a los objetivos del país, permitan generar círculos virtuosos entre la academia, la industria y el sector público, **no existe un Plan de Acción que permita articular a los actores.**

• Relaciones de cooperación con países avanzados y colaboración internacional en el marco de la Organización de los Estados Americanos (OEA) se encuentran en una fase incipiente, con prácticas y desarrollos iniciales.

• Redes de colaboración regional/internacional en ciberseguridad incipiente.

• No se reportan métricas para medir el rendimiento de la I+D del País.

• No existen programas de I+D en ciberseguridad integrados en la estrategia/política nacional.

• No hay medición del impacto de los proyectos en la industria nacional.

• No hay Indicadores de desempeño para el financiamiento y uso de recursos en I+D en ciberseguridad.

La visión de la submesa de IAC el año 2022 se resume en que:

"Cada investigador en ciberseguridad en Chile debe tener acceso a infraestructura, recursos, espacios de visibilización y colaboración que le permitan generar I+D alineado a las necesidades del País con el fin de que Chile se posicione como un actor relevante en esta materia a nivel regional dentro de los próximos 10 años."

Al apoyar a los investigadores, así como a la formación de capacidades en investigación, no solo se fortalece la innovación y desarrollo tecnológico del país, sino que también se promueve un entorno más seguro y resiliente en el ámbito digital. Este apoyo, de ser sostenido, debiera contribuir al cierre progresivo de las brechas actuales en los próximos 3 años, lo que debiera posicionarnos en el nivel "establecido".

En el año 2022, la submesa de IAC identificó cinco pilares fundamentales para alcanzar la visión de I+D en ciberseguridad en Chile:

Pilar 1: Capacidades de Investigación

Se observa desconocimiento respecto de si se realiza investigación avanzada en ciberseguridad y cuáles son los desafíos prioritarios en Chile respecto de la materia. Para subsanar estas brechas, se propuso el **Centro Nacional de Investigación en Ciberseguridad,** cuyo objetivo era consolidar un centro de desarrollo de capacidades cibernéticas que sea referente en la región.

Este centro permitiría que equipos de investigadores colaboren para abordar desafíos y amenazas prioritarias, uniendo a nuevos investigadores y reduciendo brechas de entrada.

Pilar 2: Capacidades de Innovación, Desarrollo Tecnológico Aplicado y Negocios

Se detectó una falta de integración entre investigadores y proyectos colaborativos academia-público-privado, así como la necesidad de escalar desarrollos tecnológicos al mercado. Para abordar estas brechas, se propuso el **Centro de Escalamiento y Nuevos Negocios** en torno a Resultados de Investigación en Ciberseguridad. Este centro en su concepción facilita el desarrollo de la industria de productos y servicios de base científico-tecnológica en ciberseguridad, uniendo a investigadores en proyectos colaborativos nacionales e internacionales, incubando y escalando desarrollos al mercado.

Pilar 3: Capacidades en Infraestructura y Recursos

La falta de infraestructura para investigación en ciberseguridad y la necesidad de optimizar recursos para diferentes industrias fueron identificadas como brechas críticas. Para solucionarlas, se propuso el **Laboratorio Nacional Distribuido para la I+D en Ciberseguridad,** cuyo objetivo principal radica en la generación y habilitación de infraestructura compartida para investigar, desarrollar y probar algoritmos, modelos y productos de ciberseguridad. Este laboratorio generaría los insumos para levantar requerimientos y canalizar los recursos disponibles, de manera de prever amenazas futuras en Ciberseguridad y facilitará, entre otros, la postulación conjunta a fondos concursables.

Pilar 4: Capacidades de Coordinación

Se identificó la falta de coordinación para la red de centros de investigación y escalamiento que han nacido en el país a partir de grupos de investigación emergentes y de manera incipiente, así como la falta de coordinación con diferentes organismos del Estado. Para abordar estas brechas, se propuso el **Instituto Nacional de Ciberseguridad,** cuyo objetivo era posicionar la innovación, la investigación aplicada y el desarrollo tecnológico en ciberseguridad como habilitante para el desarrollo de la economía digital y tecnológica de Chile. Este instituto tendría entre otras funciones la de coordinar la red de centros de investigación, el monitoreo de la red para medición y evaluación de desempeño, así como colaborar con el cumplimiento de la Política Nacional de Ciberseguridad, facilitando el avance de la I+D en Ciberseguridad en Chile.

Pilar 5: Capacidades de Difusión/Colaboración Internacional

La falta de visibilidad de los resultados de investigación a nivel internacional y la necesidad de fortalecer la colaboración internacional en ciberseguridad fueron identificadas como brechas. Para solucionarlas, se propuso el **Foro Nacional de Ciberseguridad, Capítulo I+D en ciberseguridad,** cuyo objetivo era entre otros establecer y fortalecer a Chile en el círculo de difusión y colaboración internacional de investigación en ciberseguridad. Este foro daba visibilidad a los resultados de investigación, posicionando a Chile en debates internacionales y generando nuevas alianzas.

→Avance de acciones que tributan a los objetivos definidos por la submesa IAC

Visibilizar a los investigadores en ciberseguridad en el país del pilar 1: Capacidades de investigación el Ministerio de Ciencias, Tecnología, Conocimiento e Innovación en colaboración con el Ministerio del Interior en Junio 2024 se lanzó el Reporte Capacidades I+D.

Tech & Negocios

Gobierno define prioridades para investigación y desarrollo en ciberseguridad

Informe de los ministerios de Ciencia e Interior determinó que las áreas prioritarias en estas materias son inteligencia artificial, criptografía, seguridad y educación.

Por: **Marco Zecchetto** | Publicado: Miércoles 12 de junio de 2024 a las 04:00 hrs.

CIBERSEGURIDAD · TRANSFORMACIÓN DIGITAL · GOBIERNO · MARCO ZECCHETTO

Romina Torres, académica UAI y Carolina Gainza, subsecretaria de MinCiencia.

Fuente: Diario Financiero, Miércoles 12 de Junio de 2024. Disponible vía web en: Gobierno define prioridades para investigación y desarrollo en ciberseguridad | Diario Financiero (df.cl)

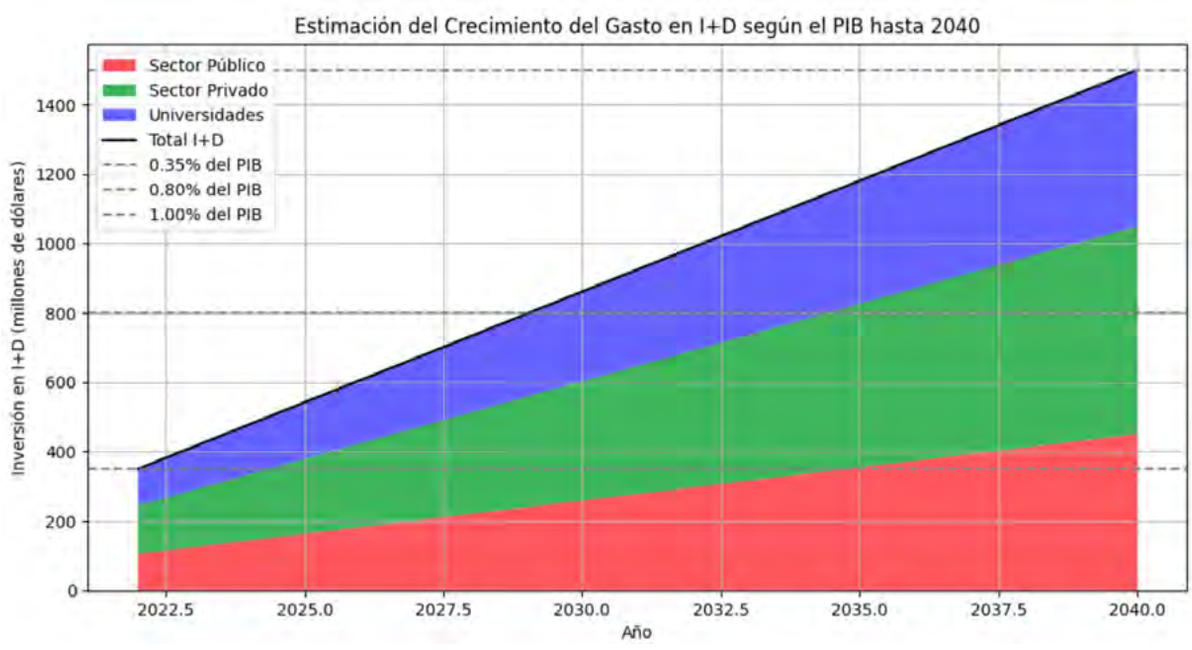
Junio 2024 fue presentado el Informe **"I+D en ciberseguridad"** generado por el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación y Ministerio del Interior, donde se realizó un levantamiento de las publicaciones en revistas indexadas por científicos con afiliación chilena durante los últimos 10 años, mostrando que existen actividades de Investigación en ciberseguridad en el País internamente pero también con redes internacionales. Por ejemplo, al menos el 50% de las publicaciones eran de conferencia lo que consideraba ponencia de estos trabajos en eventos o congresos de I+D en ciberseguridad internacionales.

Este informe presentó además cuatro áreas de investigación en las que se sugiere que los investigadores deben seguir profundizando: Criptografía post cuántica, Desarrollo seguro de sistemas ciber físicos, Sinergia bidireccional entre IA y ciberseguridad, y Educación.

En sincronía con el aumento de madurez en el factor D3.4, el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación estudia alternativas dentro de la diversidad de los instrumentos de la Agencia Nacional de Investigación y Desarrollo, instrumentos "prioritario" para ciberseguridad (ejemplo: adición permanente de temática ciberseguridad a FONDEF I+D)

Fuente: Sofofa 18 04 2023 FINAL.pdf De la crisis a la normalización: la economía chilena en tres tiempos, Ministerio de Hacienda, Abril 2023

Según la proyección del crecimiento del PIB realizada por el Banco Central en el período 2024- 2050, así como el Plan de Gobierno «Invirtamos en Chile», la generación de estímulos para la inversión, en particular los destinados al sector de la ciencia y la tecnología, deberá incrementarse del 0,35 % actuala un 1 % en el 2040, con un impacto del 50 % de participación del sector privado en el 2030, una vez que se alcance el 0,8 % de gasto en I+D, es decir, un 0,4 % procedente de las alianzas público-privadas para la inversión, junto con una mejora en el acceso a programas de financiación y a la inversión extranjera directa. Esto permite visualizar un escenario en el que el ecosistema participa en partes iguales en la generación de recursos para la I+D, en particular en ciberseguridad. Esto último es extrapolable a los escenarios derivados de las proyecciones de necesidades de generación de conocimiento en ciberseguridad, como eje estratégico de importancia en la transferencia hacia el sector público-privado.



Fuente: Sofofa 18 04 2023 FINAL.pdf De la crisis a la normalización: la economía chilena en tres tiempos, Ministerio de Hacienda, Abril 2023

En el contexto del presente trabajo, se realizó un Diagnóstico de áreas críticas desde la mirada de los Investigadores Independientes en Seguridad de la Información. Para llevar a cabo el diagnóstico, se realizaron distintas entrevistas con investigadores independientes en diversas regiones de Chile. Se identificaron y analizaron casos específicos en áreas críticas como la criptografía, los ataques patrocinados por estados, la seguridad en la defensa nacional y los riesgos tecnológicos asociados a las vulnerabilidades humanas.

→Contexto General

Los investigadores entrevistados comparten un perfil similar en cuanto a su independencia, autosuficiencia financiera y dedicación a temas de alta relevancia en ciberseguridad. A pesar de la falta de apoyo estatal o en conjunto con alguna institución, han logrado avanzar en sus investigaciones sin poder publicar u ofrecer su investigación a sujetos de interés. Sus proyectos no solo abordan amenazas técnicas, sino también problemas sociales y éticos relacionados con el uso de la tecnología.

→Temáticas de Investigación

Las áreas de enfoque de estos investigadores son diversas, lo que resalta la amplitud de la ciberseguridad como disciplina. Entre sus principales líneas de investigación encontramos:

- **Criptografía Post Cuántica y Ransomware Educativo**
- **Algoritmo de Cifrado para Defensa Nacional**
- **Ataques Patrocinados por Estados**
- **Riesgos Tecnológicos utilizando vulnerabilidades humanas**

Cada uno de estos temas aborda aspectos críticos de la ciberseguridad, desde la protección de infraestructura crítica hasta la educación y prevención de riesgos en menores. El enfoque multifacético de estas investigaciones refleja la complejidad de las amenazas actuales y futuras.

→Desafíos Financieros y Barreras Institucionales

Uno de los principales problemas que comparten los entrevistados, es la falta de financiamiento adecuado. Todos los proyectos se financian de manera independiente, lo que ha llevado a la suspensión o retraso de varias investigaciones. Destacan además, que las barreras para acceder a fondos estatales o a apoyos institucionales dificultan el desarrollo a largo plazo de iniciativas en I+D, especialmente en áreas tan complejas y cambiantes como la ciberseguridad.

El hecho de que estos investigadores se autofinancien limita su capacidad de expansión y colaboración. Algunos de ellos han señalado que, aunque logran completar investigaciones preliminares, la falta de recursos impide su mejora continua o adaptación a nuevas tecnologías y necesidades emergentes.

→Innovación y Contribución a la Ciberseguridad

A pesar de los obstáculos financieros, estos investigadores están desarrollando soluciones innovadoras en sus respectivas áreas. Cada uno, espera poder contribuir de forma significativa a nivel local

- El uso de la criptografía post cuántica para la evasión de sistemas demuestra cómo las nuevas tecnologías pueden superar las barreras tradicionales en la detección de amenazas. Además, el enfoque educativo del ransomware permite que tanto expertos como principiantes comprendan mejor estos procesos.

- El desarrollo de algoritmos de cifrado avanzado orientado a la protección de información secreta refuerza la seguridad de infraestructuras críticas, especialmente en el ámbito de la defensa.

- La capacidad de rastrear y realizar ingeniería inversa a ataques patrocinados por estados destaca la importancia de entender no solo las amenazas técnicas, sino también los actores detrás de ellas.

- El enfoque pedagógico en la investigación sobre los riesgos de la manipulación de las personas y, por sobre todo, del uso no controlado de la tecnología en menores es clave para la prevención de problemas sociales derivados del uso indebido de internet y dispositivos.

→Potencial no Aprovechado y Futuro de la Investigación Independiente

El análisis del trabajo de investigación desarrollado, destaca el potencial no aprovechado de la investigación independiente en ciberseguridad como una necesidad urgente que requiere generar mecanismos de apoyo financiero y apoyo tecnológico para investigadores autónomos. A pesar de su ingenio, creatividad y aportes al campo, el progreso de sus investigaciones se ve limitado por la falta de recursos. Es necesario proporcionar apoyo a estos investigadores, con esto, no solo podrían completar, publicar, mantener y presentar sus proyectos, sino también contribuir a la formación de futuras generaciones de expertos en ciberseguridad.

→Análisis de Instituciones Públicas y Privadas en Ciberseguridad

Este análisis se centra en instituciones, tanto públicas como privadas, que desempeñan un papel importante en la educación, concientización y gestión de la ciberseguridad a nivel nacional. A pesar de no estar dedicadas a la investigación en ciberseguridad como los investigadores independientes mencionados previamente, estas instituciones cumplen de relevancia en la protección digital, formación educativa y desarrollo de capacidades tecnológicas para enfrentar las amenazas cibernéticas. Se destaca la colaboración entre los sectores público, privado y académico como un factor clave para avanzar en la investigación y la gestión de riesgos cibernéticos.

Las instituciones con quienes se ha tenido conversaciones tienen enfoques variados, desde la educación y concientización sobre la ciberseguridad, hasta el análisis forense de delitos digitales. Aunque solo una de las instituciones está vinculada directamente a la investigación tecnológica, todas juegan un papel esencial en la formación y protección digital de la ciudadanía. Los objetivos de cada una van desde el nivel local hasta el internacional, con diversos grados de influencia y especialización.

Algunas instituciones se centran en la educación y concientización en ciberseguridad, con un enfoque en el uso seguro de internet y la formación de ciudadanos digitales, especialmente en jóvenes y niñas.

Una organización sin fines de lucro que se financia principalmente por aportes del sector empresarial. Sus esfuerzos están orientados a la educación sobre ciberseguridad, destacando los talleres de "Futuro de la Educación", con un fuerte énfasis en la ciudadanía digital para estudiantes de enseñanza media. Esta organización tiene un impacto nacional con base en Santiago.

Esta fundación, con presencia en múltiples ciudades del país, ofrece un taller de protección digital como parte de su programa de capacitación para niñas, así como una campaña de concientización a la población general. Su labor, mayoritariamente apoyada por voluntarios, busca expandirse a más regiones del país, proyectando nuevas participaciones en Puerto Montt y Rancagua.

Otra institución, aunque no realiza investigación científica en ciberseguridad, tiene uno de los roles de mayor impacto en la aplicación de la ley y la gestión de delitos cibernéticos a nivel nacional. Este departamento está enfocado en la investigación forense digital, desarrollando proyectos que responden a las demandas de delitos específicos.

Este organismo especializado en el análisis de cibercrimen tiene presencia física en 3 regiones del país, con un enfoque en la investigación forense digital y está en diseño un nuevo equipo destinado a la investigación de delitos en internet y malware. Sin embargo, la naturaleza delicada de la información con la que trabajan les impide colaborar abiertamente con otros sectores. Además, han encontrado dificultades para establecer relaciones con el mundo académico, lo que limita su capacidad de avanzar en investigación y desarrollo.

La cuarta institución pública, aunque no realiza investigación directa, desempeña un rol estratégico al sentar las bases para el desarrollo de la investigación e innovación en tecnología, particularmente en ciberseguridad.

Esta entidad estatal tiene bajo su alero el informe I+D en Ciberseguridad, y trabaja en la creación de "anillos de conocimiento", teniendo uno de estos anillos el enfoquen en ciberseguridad. Su objetivo es fortalecer la investigación a nivel nacional a través de la administración de fondos y conocimientos.

→Desafíos y Oportunidades

Un desafío compartido entre estas instituciones es la dificultad para crear una colaboración efectiva entre los sectores público, privado y académico. Si bien cada entidad trabaja en su respectivo campo de ciberseguridad, la falta de integración y cooperación limita la capacidad de avanzar en investigaciones conjuntas o en la creación de soluciones tecnológicas más avanzadas.

Aunque algunas instituciones, como la primera, cuentan con apoyo del sector empresarial, otras dependen en gran medida del voluntariado o carecen de los recursos suficientes para realizar investigación propia. Esto es especialmente evidente en las instituciones que no tienen un enfoque directo en I+D, pero que aún necesitan expandir sus capacidades para enfrentar amenazas cibernéticas más sofisticadas.

El llamado de la tercera y cuarta institución a establecer alianzas entre los sectores público, privado y académico es un punto crucial para superar las barreras actuales. La creación de redes colaborativas podría facilitar el acceso a nuevos recursos, conocimientos especializados y apoyo tecnológico, lo que permitiría avanzar más rápidamente en la investigación y desarrollo en ciberseguridad.

→Papel Fundamental en la Educación y Protección Digital

Las instituciones, hasta ahora, analizadas juegan un rol fundamental en la ciberseguridad nacional, ya sea a través de la educación y concientización, o en la gestión y análisis de delitos digitales. Sin embargo, existe una necesidad urgente de mejorar la colaboración entre estas entidades y otros actores del ecosistema de ciberseguridad para maximizar el impacto de sus esfuerzos. El futuro de la ciberseguridad en Chile depende en gran medida de la capacidad de estas instituciones para unir fuerzas y trabajar hacia un objetivo común, la protección integral de los usuarios, sistemas digitales y la defensa nacional en el ciberespacio.

→Acciones derivadas de la implementación de la Política Nacional de Ciberseguridad PNC 2023-2028

El trabajo del foro en la Dimensión 3.4 también considera la Política Nacional de Ciberseguridad (PNC) actual 2023-2028 - respecto a investigación en Ciberseguridad, en donde establece que:

La nueva Política Nacional de Ciberseguridad de Chile para el período 2023-2028 incluye diversos objetivos estratégicos, uno de los cuales se relaciona con la investigación, desarrollo e innovación (I+D+i) en ciberseguridad, siendo los restantes el desarrollo de infraestructura resiliente, la protección de los derechos de las personas, el fomento a una cultura de Ciberseguridad y la coordinación nacional e Internacional. Se busca, por lo tanto, **promover el desarrollo de una industria de ciberseguridad que proteja a las personas y organizaciones y que sirva a los objetivos estratégicos del país.**

Para ello, se fomentará la investigación científica aplicada en temas de ciberseguridad, acorde a las necesidades del país, entre las cuales se cuentan:

- Aumento de Resiliencia de las Organizaciones en Infraestructura del País,

- Desarrollo de Cultura de Ciberseguridad de Organizaciones y Personas,

- Incremento de especialistas en Ciberseguridad y formación de Capital Humano Avanzado en Ciberseguridad

- Necesidad de incremento en sofisticación de capacidades en Ciberseguridad para cubrir la demanda de soluciones tecnológicas

- Necesidad de mejorar la protección de la Sociedad Chilena ante el incremento de la sofisticación de delitos tecnológicos.

En lo que concierne al Fomento a la Industria y la Investigación Científica como objetivo de la PNC 2023-2028, se indica que "El país promoverá el desarrollo de una industria de la ciberseguridad, que proteja a las personas y las organizaciones y que sirva a sus objetivos estratégicos. Este fomento se implementará a través de estímulos y fondos dirigidos a la oferta de servicios y productos en ciberseguridad, pero también a través de la generación de una demanda más sofisticada en ciberseguridad, de forma que nuestra industria pueda proteger de mejor forma a las personas y organizaciones, y servir mejor a los intereses del país".

Lo anterior, teniendo en consideración que las prioridades de la PNC se centran en la Cooperación Internacional y el Desarrollo de Capacidades, a lo que se suma la existencia de una Política Nacional de Inteligencia Artificial, así como una Política Nacional contra el Crimen Organizado.

Para avanzar en este objetivo, es necesario:

1.Focalizar la investigación aplicada respecto a aquellos problemas y necesidades en ciberseguridad tanto del sector público como privado. Para ello, se promoverá la **creación de institutos de investigación científica aplicada y transferencia tecnológica** en la materia, con la finalidad de que potencien la ciberseguridad como un área **preferente** por parte del sector académico nacional, y que conecten las necesidades de las organizaciones y el sector público con el conocimiento científico existente.

2.Generar incentivos para el emprendimiento tecnológico en ciberseguridad, impulsado por las necesidades de las organizaciones privadas y públicas de nuestro país, particularmente por los Centros de Respuesta a Incidentes de Seguridad Informática (CSIRTs), al alero de grupos de investigación en universidades y centros de investigación. Estos incentivos no se restringirán al ámbito económico, serán amplios y se enfocarán especialmente en las regiones del país distintas de la Región Metropolitana.

3.Revisar los mecanismos de contratación de servicios de ciberseguridad por parte del Estado, para hacerlos más eficientes y expeditos, dando preferencia a la contratación de servicios de ciberseguridad ofrecidos por la industria local.

4.Promocionar los productos y servicios de las empresas locales en ciberseguridad a nivel nacional y en el extranjero, a través de fondos públicos y alianzas público-privadas, y generar incentivos económicos y tributarios para que las empresas existentes puedan ampliar su oferta de servicios en ciberseguridad y ofrecerla de forma preferente al Estado.

5.Fomentar la integración e inclusión de una transversalización de género en el desarrollo del ecosistema de ciberseguridad en nuestro país, generando medidas de acción positiva que permitan aumentar el número de mujeres en roles gerenciales y técnicos en ciberseguridad.

Lo anterior, significa que desde la mirada del Foro D3.4, en lo concerniente a la Investigación e Innovación en Ciberseguridad del País, se requerirá de:

• Incentivar la **inversión público - privada** en el área de ciberseguridad y estimular la colaboración con instituciones de educación superior y centros de investigación nacionales, para el desarrollo, uso e implementación intensiva de nuevas tecnologías.

• Promover la creación de institutos de **investigación científica aplicada y transferencia tecnológica** en la materia, con la finalidad de que potencien la ciberseguridad como un área preferente por parte del sector académico nacional, y que conecten las necesidades de las organizaciones y el sector público con el conocimiento científico existente.

• Generar **incentivos para el emprendimiento tecnológico en ciberseguridad,**

• **Promocionar los productos y servicios de las empresas locales en ciberseguridad a nivel nacional y en el extranjero,** a través de fondos públicos y alianzas público- privadas, y generar incentivos económicos y tributarios para que las empresas existentes puedan ampliar su oferta de servicios en ciberseguridad.

→Situación Futura: Nivel de madurez establecido en el Factor D3.4

Con los elementos presentados, tanto históricos como presentes, y bajo la hipótesis que la medición, según el Modelo de Oxford que se efectuará este año respecto del Dominio D3.4, nos ubicará como país en el nivel "formativo", se desprende que para alcanzar el nivel de madurez "establecido" a 4 años en materias de IAC, y en concordancia con la PNC 2023-2028, tanto la Estrategia Nacional de Ciberseguridad que se derive como el Plan de Acción que la acompañe, deberá contener explícitamente, al menos lo siguiente:

- Catastro actualizado de actividades de IAC que se realizan en el País y con países socios,

- Catastro de Recursos y Procesos requeridos para realizar las actividades de IAC,

- Catastro de fuentes actuales de financiamiento disponibles que resulten adecuadas para realizar estas actividades,

- Catastro de actores regionales e internacionales del ámbito público y privado con los que se realiza investigación científica, además de mostrar evidencia de la existencia y operación de redes de colaboración regional/internacional con prácticas y desarrollos,

- Métricas y sus valores que permitan evaluar y medir el rendimiento de las acciones de IAC y su evolución temporal.

Notamos también que, sin embargo, aunque la PNC 2023-2028 menciona la promoción de la investigación científica aplicada en ciberseguridad, no es explícita en cuanto su carácter estratégico nacional, ni a las métricas específicas propuestas para medir el rendimiento y progreso de las acciones de I+D+i.

Por tanto estimamos que en el corto plazo se necesita:

1. Especificar las áreas prioritarias de investigación y los tipos de proyectos de I+D+i que, por su carácter y naturaleza estratégicas, se deben fomentar.

2. Diseñar y poner a disposición un Plan detallado de los recursos (RRHH, Tecnológicos) así como de los Procesos específicos necesarios para dar adecuado curso a dichas actividades.

3. Identificar claramente las fuentes de financiamiento disponibles, tanto nacionales como internacionales para I+D+i en Ciberseguridad, y los mecanismos requeridos para acceder a ellas.

4. Especificar concretamente los actores Regionales e Internacionales que se visualizan para colaboración en I+D+i.

5. Finalmente, las Métricas que se precisan para mejor evaluación del rendimiento de las acciones de I+D+i, así como un sistema de seguimiento y reporte del progreso.

En resúmen, la PNC 2023-2028 contiene los elementos de base para alcanzar el nivel de madurez “establecido” en I+D+i en ciberseguridad, pero necesita ser más explícita en ciertos aspectos para asegurar el éxito. Al detallar las actividades, recursos, financiamiento, colaboración y métricas, la política puede proporcionar una guía más clara y efectiva para avanzar en el camino hacia la madurez en esta área crítica para la Soberanía Digital del País.

Para ello la próxima subsección explicita un posible plan de acción.

→Actualización del Plan de Acción de Actividades Prioritarias, Iniciativas para asegurar la investigación avanzada en Chile

El análisis del Foro sobre el camino hacia la madurez en investigación e innovación en ciberseguridad para Chile, basado en el texto “Construyendo la Ciberseguridad en Chile”, revela que, si bien se han dado pasos importantes en el ámbito legislativo y de gobernanza, aún existen áreas críticas para que el país logre una madurez avanzada en investigación e innovación en ciberseguridad. Para abordar dichas áreas, proponemos el siguiente Plan de Acción 2023-2028:

1. Actividades Prioritarias:

a. Fortalecimiento del Ecosistema de Investigación y Desarrollo (I+D) en Ciberseguridad

b. Creación y Fortalecimiento de Alianzas Público-Privadas y Colaboración Internacional

c. Formación de Investigadores en Ciberseguridad y fortalecimiento de la Academia

d. Contribución a la Cultura de Investigación e Innovación en Ciberseguridad

2. Programas:

a. Inversión Público-Privada para I+D+i

b. Desarrollo de Centros de Innovación

c. Formación, Captación y Retención de Capital Humano Avanzado en Ciberseguridad

3. Proyectos:

a. Fomento de la Ciber Higiene y la Innovación desde la Base

b. Construcción de Comunidades de Interés

4. Métricas y Evaluación de Progreso en I+D:

a. Indicadores Clave de desempeño (KPI)

b. Evaluación continua de amenazas emergentes

El análisis de base para la elaboración de este plan de acción gravita en torno a los cinco pilares siguientes: Capacidades de Investigación, Capacidades de Innovación, Desarrollo Tecnológico Aplicado y Negocios, Recursos de Infraestructura, Capacidades de Coordinación: Cultura y Normativas, y finalmente Capacidades de Difusión/Colaboración Internacional. Estos cinco pilares se describen a continuación, desagregados por objetivos específicos, iniciativas involucradas, indicadores de desempeño KPI y sus salidas esperadas.

Pilar 1: Capacidades de Investigación

Programa: Centro Nacional de Investigación en Ciberseguridad:

→Objetivo macro: Consolidar las actividades de investigación avanzada, proporcionando un marco estructurado para la I+D en ciberseguridad.

OE	Iniciativas	KPI	Salidas Esperadas
[OE1] Identificar áreas prioritarias relevantes actuales, emergentes y futuras en Ciberseguridad susceptibles de ser abordadas mediante Investigación Avanzada.	[I16.S7] Generar Dashboard Web Anual de amenazas futuras y riesgos emergentes en ciberseguridad. Generar las comunidades de IAC en: [I5.1.S10] Machine Learning Poisoning [I5.2.S1] Optimización de capacidades de detección [I5.3.S10] Criptografía (Cuántica y Postcuántica) [I5.4.S10] Interoperabilidad	Nro de áreas de trabajo en IAC Nro de riesgos emergentes en ciberseguridad del año anterior, actual o futuro reconocida como prioritaria para el País Nro de iniciativas generando IAC en amenazas futuras. Nro publicaciones Scopus/Wos Nro Datasets liberados % de amenazas abordadas	[S7] Reporte Anual de Estudio de áreas prioritarias relevantes actuales, emergentes y futuras en Ciberseguridad susceptibles de ser abordadas.

OE	Iniciativas	KPI	Salidas Esperadas
[OE2] Aumentar la cantidad de investigadores en áreas relevantes y prioritarias	[I5.5.S10] Identidad digital con biometría [I5.6.S10] Fake News [I5.7.S10] Resiliencia en infraestructura Crítica / IIoT [I5.8.S10] Investigación Forense Digital [I5.9.S11] Ciudades Inteligentes y subcomunidades (e.g. Smart Health) [I5.9.S12] Regulaciones y Legislación. [I5.9.S13] Ciberseguridad por Diseño [I5.9.S14] Privacidad por diseño [I14.S10] Generar Prácticas de IAC en áreas de investigación en ciberseguridad [I1-S1]Levantar Catastro nacional de investigadores en ciberseguridad	% de riesgos emergentes abordados Nro Herramientas Liberadas Nro de capacitaciones Nro Instancias de divulgación realizadas Nro de citas a publicaciones Nro de proyectos en lso que participa la comunidad financiados por ANID Nro de proyectos en los que participa la comunidad financiados Nro de proyectos o en colaboración con organismos públicos Nro de proyectos o en colaboración con organismos privados Nro de proyectos en colaboración internacional % de comunidades activas	[S10] Comunidades de IAC en áreas relevantes a nivel País.

OE	Iniciativas	KPI	Salidas Esperadas
[OE3] Visibilizar a los investigadores en ciberseguridad en el País	[I3-S1] Levantar catálogo indexado sobre github de los papers/ tesis/reportes, códigos y datasets que se están generando en Chile	% de investigadores reconocidos actualizando información en plataforma anualmente Tasa de investigadores vs aporte a catalogo indexado Nro de aportes en catálogo por tipo % de uso del catálogo	[S1] Catastro de Investigadores Nacionales con Actividad en IAC
[OE4] Posibilitar y facilitar el ingreso de investigadores al área. (por ej, asociar ANID, Corfo, etc.) mediante la Identificación y/o propuesta, gestión y difusión de programas y marcos presupuestarios de fomento a la IAC	[I6.S6] Generar Concurso Becas para Doctorados académicos científicos en IAC multidisciplinar (otras disciplinas) [I7.S6] Generar Concurso Becas para Doctorados académicos científicos en IAC en sectores específicos (e.g. Minería) [I10.S9] Crear Grupo de Estudio y Definición de Estándares, procedimientos y guías en IAC. [I19.S11] Generar programa de IaaS para que investigadores puedan correr experimentos	Nro de nuevos investigadores financiados indirectamente con los mecanismos % satisfacción de guía % de oportunidades de mejora de la guía abordados por investigadores y cerrados satisfactoriamente por la comunidad Nro de investigadores beneficiados por starterkits Nro de investigaciones con reconocimiento a estos instrumentos. Nro de becados en IAC % de becados en IAC no técnico.	[S6] Programas académicos científicos en Ciberseguridad con foco en formación de investigadores en el área [S9] Guía para realizar investigación avanzadas en ciberseguridad [S11] Starter Kit de Infraestructura habilitante para realizar IAC

OE	Iniciativas	KPI	Salidas Esperadas
[OE5] Fomentar la creación de Redes de Investigación Colaborativas para Ciberseguridad intra país, interorganismos, a nivel regional e internacionalmente.	[I1-S1-S2]Levantar Catastro nacional de investigadores en ciberseguridad [I2-S8] Levantar Catastros de Centros de investigación colaborativa intersectorial alrededor de la ciberseguridad [I4.S4] Levantar Plataforma de desafíos de IAC de manera interdisciplinaria [innovación abierta] [I9.S4]Generar Concurso ANID Instituto Milenio/ centros/Núcleo de Investigación con llamado a la Ciberseguridad, [I11.S4] Generar Concursos ANID/Corfo asociado a Fondef Idea/ Tecnológico temático en ciberseguridad [I12.S4] Crear Centro Nacional de Investigación en Ciberseguridad (no adscrito o bajo el alero de una Universidad o Consorcio Universitario) Institución gubernamental similar al INRIA (Francia) -	Nro de redes de colaboración existentes % de investigadores participando en redes de IAC nacional % de investigadores participando en redes de IAC internacional Nro proyectos científicos tecnológicos en IAC % proyectos científicos tecnológicos en IAC con integrantes multidisciplinarios % proyectos científicos tecnológicos en IAC con integrantes internacionales % proyectos científicos tecnológicos en IAC con al menos 50% integrantes de regiones diferentes a la RM % investigadores de IAC chilenos fuera de Chile Nro desafíos levantados en plataforma de innovación abierta %desafíos que consideran demandantes públicos %desafíos que consideran demandantes privados	[S2] Catastro de Redes de Colaboración de Ciberseguridad dedicadas a la Investigación Avanzada [S8] Catastro de Redes de Investigación Colaborativas para Ciberseguridad intra país, interorganismos, a nivel regional e internacionalmente. [S4] Programas de Proyectos colaborativos científicos-tecnológicos en Ciberseguridad nacional-internacional-multidisciplinario

OE	Iniciativas	KPI	Salidas Esperadas
[OE4] Posibilitar y facilitar el ingreso de investigadores al área. (por ej, asociar ANID, Corfo, etc.) mediante la Identificación y/o propuesta, gestión y difusión de programas y marcos presupuestarios de fomento a la IAC.	Consolidar en Chile un centro de desarrollo de capacidades cibernéticas que sea referente en la región en investigación avanzada en materias de ciberseguridad en sus diversas áreas de especialización. [I13.S4] Crear Programa de importación de expertos internacionales (concurso ANID) [I8.S5] Generar Concurso Becas para pasantías de investigadores en centros de IAC internacionales. [I14.S5] Generar Prácticas de IAC en áreas de investigación en ciberseguridad. [I15.S5] Generar Programa de Pasantías en Centros Nacionales de Investigación en Ciberseguridad Fomentar instancias de pasantías para estudiantes de pre y post grado en la industria nacional e internacional y en entidades gubernamentales para acelerar el desarrollo de capacidades tecnológicas en el país.	Nro de PoC generadas para desafíos expuestos en muestras Nro de núcleos Institutos en IAC Nro de proyectos fondecyt en IAC Nro de proyectos FONDEF en IAC Nro de expertos internacionales con estadías superiores a las dos semanas en Chile por iniciativas de las redes de IAC Nro de investigadores seniors beneficiados en pasantías en centros de IAC internacional. Nro de investigadores jr beneficiados en pasantías en centros de IAC nacional Nro de profesionales estudiantes beneficiados para realizar prácticas.	[S5] Programas de Formación de Capital Humano Avanzado en colaboración internacional.
[OE6] Desarrollar métricas y estándares a nivel nacional para aumentar la madurez de las investigaciones avanzadas en ciberseguridad	[I17.S3] Generar Mecanismo de monitoreo y Control para indicadores de la IAC que se realiza en Chile.	% de métricas en visibles actualizados en dashboard	[S3] Set de métricas con valores base periodo 2023-2035.

Pilar 2: Capacidades de Innovación, Desarrollo Tecnológico aplicado y Negocios

→Centro de Escalamiento y Nuevos Negocios en torno a Resultados de Investigación en Ciberseguridad

OE	Iniciativas	KPI	Salidas Esperadas
OE-PNC5 [Estimular] Generación de demanda de parte del sector público basado en los intereses estratégicos del Estado	Generar Estudio de caracterización de Industria.	% Aumento del Tamaño del sector TIC debido a IAC.	Estudios tanto de caracterización de la industria de ciberseguridad (oferta), como de acceso y uso de ciberseguridad en el país (demanda), con el objeto de orientar programas especiales para impulsar la industria de ciberseguridad nacional, en sectores definidos.
	Generar Eventos de brainstorming para generación de ecosistemas en IAC.	N° de Empresas o Startups de base científica-tecnológica chilenas que ofrecen o desarrollan productos o servicios de ciberseguridad para la industria local o internacional.	
	Generar material para difusión y capacitación de mejores prácticas para convertir investigación aplicada en ciberseguridad en productos de base científica tecnológicas insertados exitosamente en la Industria.	No de participantes relevantes en eventos	Eventos de difusión para generar concientización y networking en el ecosistema referido a los desafíos y desarrollos en ciberseguridad.
	Programa de fortalecimiento de la Industria de la ciberseguridad.		Una o más instancias de colaboración multisectoriales con diversos actores sociales (ONG, empresas, gremios, academia y otras)
	Generar Alianzas importantes entre organismos de seguridad interior y defensa exterior con la industria nacional en el área.		
	Generar Programa de emprendimiento en ciberseguridad		

OE	Iniciativas	KPI	Salidas Esperadas
OE-PNC2 Facilitar el desarrollo de la industria de productos y servicios de base científica-tecnológica en el área de ciberseguridad en Chile	Levantar Plataforma de desafíos de IAC de manera interdisciplinaria.	N° de Empresas o Startups de base científica-tecnológica chilenas que ofrecen o desarrollan productos o servicios de ciberseguridad para la industria local o internacional. Nro de proyectos activos para fortalecer la ciberseguridad en cierto sector industrial por medio de la IAC multidisciplinaria	
	Desarrollar concursos para el desarrollo de investigación por encargo en el área de ciberseguridad que requieran de la colaboración Universidad-Industria.		
	Desarrollo de incentivos a la colaboración startup-empresa.		
	Desarrollo de laboratorios de pruebas de concepto en el área de ciberseguridad.		
	Impulsar un Desafío de Innovación Pública (iniciativa conjunta entre ANID y Laboratorio de Gobierno) en ciberseguridad.		
	Convocatoria a Programa de escalamiento y nuevos negocios en torno a resultados de investigación en ciberseguridad (CORFO ANID)		
	ANID Proyectos cooperacion internacional a través de PCI (Programas de Colaboración Internacional) con recursos para Networking.		

OE	Iniciativas	KPI	Salidas Esperadas
OE-PNC3 - Desarrollar modelos de colaboración que permitan el avance del desarrollo de tecnología en ciberseguridad desde las etapas experimentales de la investigación aplicada hacia niveles de TRL maduros que permitan la salida al mercado.	Levantar Plataforma de desafíos de IAC de manera interdisciplinaria.	% de Aumento del Tamaño del sector TIC debido a IAC.	Modelos de innovación abierta en IAC
	Desarrollar concursos para el desarrollo de investigación por encargo en el área de ciberseguridad que requieran de la colaboración Universidad-Industria.	Nro de productos de IAC en al menos nivel 5	
		% de investigadores en proyectos de colaboración.	
	Desarrollo de incentivos a la colaboración startup-empresa.	Nro de productos de IAC entre 6 y 9.	
	Desarrollo de laboratorios de pruebas de concepto en el área de ciberseguridad.	Nro de proyectos establecidos luego del desafío de innovación abierta.	Modelos de innovación abierta e investigación aplicada.
	Impulsar un Desafío de Innovación Pública (iniciativa conjunta entre ANID y Laboratorio de Gobierno) en ciberseguridad	N° de pruebas de conceptos realizadas en laboratorios.	
		Nro de investigaciones realizadas por encargo donde colaboran Universidad e Industria	
OE-PNC4 Desarrollar modelos de escalamiento e internacionalización de productos y servicios nacionales en el área de ciberseguridad,	Convocatoria a Programa de escalamiento y nuevos negocios en torno a resultados de investigación en ciberseguridad (CORFO-ANID)	Nro de productos de base IAC con salida internacional.	Modelos de escalamiento Modelos de Internacionalización
		Nro de prodyctos de base IAC escalados.	
	ANID Proyectos cooperacion internacional a través de PCI (Programas de Colaboración Internacional) con recursos para Networking.		

OE	Iniciativas	KPI	Salidas Esperadas
	Presencia activa en ferias de connotación nacional e internacional para dar a conocer y posicionarse en la región a través de los desarrollos alcanzados. En este sentido, se podría analizar la participación en ferias como FIDAE, EXPOMIN, EXPONAVAL, entre otras que permitan posicionar al país como un referente en la región y a nivel global en la generación de diversas capacidades del área de la investigación avanzada en materias de ciberseguridad.	Nro de negocios alrededor de productos de base IAC	
	Fomentar instancias de pasantías para estudiantes de pre y post grado en la industria nacional e internacional y en entidades gubernamentales para acelerar el desarrollo de capacidades tecnológicas en el país.		
OE7- Facilitar el desarrollo de modelos de financiamiento e incentivos para la transición adecuada de investigación aplicada hacia el mercado.	Generar Instrumento de financiamiento para la Atracción de inversión para el crecimiento y desarrollo de la industria de ciberseguridad (ANID)	N° de licencias (u otro mecanismo de protección de propiedad intelectual) transferidas de forma efectiva para su explotación comercial.	Modelos de Financiamiento
	Generar Instrumentos de fomento al patrocinio del Estado a proyectos de I+D+i con financiamiento público o privado, nacional o internacional en materias de Ciberseguridad.	N° de instituciones participantes en iniciativas de innovación abierta en ciberseguridad con foco en desarrollo de soluciones, productos o servicios en el área.	Modelos de incentivos

OE	Iniciativas	KPI	Salidas Esperadas
	Concursos ANID/ Corfo asociado a Startup temático en ciberseguridad	Nro de doctores en IAC insertos en Industria.	
		% de doctores en IAC insertos en Industria.	
		N° de Empresas o Startups de base científica-tecnológica chilenas que ofrecen o desarrollan productos o servicios de ciberseguridad para la industria local o internacional.	
		Nro de proyectos de I+D+i de base IAC patrocinados por estado	

Pilar 3: Recursos de Infraestructura

→Laboratorio Nacional Distribuido para la I+D en Ciberseguridad: Proveerá la infraestructura compartida necesaria para investigar, desarrollar y probar tecnologías de ciberseguridad.

OE	Iniciativas	KPI	Salidas Esperadas
Habilitar una infraestructura compartida que permita investigar desarrollar y probar algoritmos/modelos/ productos del segmento ciberseguridad para diferentes Industrias optimizando recursos.	Levantar requerimientos de infraestructura existente en términos de recursos de procesamiento Identificar geográficamente potenciales nodos que permitan integrar las capacidades de investigación y desarrollo digital nacional.	Nro de proyectos e iniciativas de desarrollo e investigación por sectores (industria, gubernamental, defensa, retail, banca, etc) en materias de ciberseguridad que se enfoquen en el desarrollo nacional.	Catastro de capacidades de infraestructura (Informe estatus actual de Chile)

OE	Iniciativas	KPI	Salidas Esperadas
Desarrollar mejores prácticas en I+D en ciberseguridad en aspectos de recursos.	Visibilizar la red de infraestructura existente en términos de recursos de Procesamiento. Proyectos Fondequip Identificar mecanismos o estructuras de financiamiento que permitan asegurar la continuidad del desarrollo de capacidades en materias de ciberseguridad y sus diversas áreas de especialización. Creación de Laboratorios de Pruebas y Prototipos para proyectos con I+D en Ciberseguridad. Creación del Laboratorio nacional distribuido en ciberseguridad.	Miles de Millones en financiamiento e inversiones, generación de masa critica de especialistas y dimensión de las capacidades y desarrollo tecnológico alcanzada relativo a la ciberseguridad nacional. Nro de nodos de la red nacional de IAC Nro de nodos que proveen infraestructura Miles de millones adjudicados en Fondequip % de infraestructura mínima necesaria para IAC en diferentes ámbitos % cubrimiento de demandas de requerimiento de infraestructura Nro usuarios del Laboratorios de Pruebas y Prototipos Nro usuarios del Laboratorio Nacional Distribuido %de ocupación del Laboratorio Nacional Distribuido	Guía de las mejores prácticas para recursos y procesos requeridos para realizar actividad de IAC

OE	Iniciativas	KPI	Salidas Esperadas
Integrar la academia (universidades e institutos de educación superior), a los procesos de investigación en organizaciones gubernamentales orientado al desarrollo y optimización de los recursos digitales del país.	Oficialización de un proceso que facilite la integración de la academia a áreas de desarrollo tecnológico en organismos del Estado.	Nro convenios integración academia Estado Nro de ámbitos donde se participa en generación de capacidades de desarrollo digital e investigación	
Identificar y materializar oportunidades de inversión que contribuyan y faciliten el desarrollo de capacidades en materias de ciberseguridad de Chile.	Contar con una participación en ámbitos de investigación y generación de capacidades de desarrollo digital y cibernético a partir de proyectos de connotación nacional como lo son el Proyecto Nacional Satelital, u otros que permitan un apalancamiento entre la industria, el estado y la academia.		

Pilar 4: Capacidades de Coordinación: Cultura y Normativas

→Programa:Instituto Nacional de Ciberseguridad: Coordinará la identificación y gestión de fuentes de financiamiento, facilitando el acceso a recursos económicos para la I+D.

OE	Iniciativas	KPI	Salidas Esperadas
OE-PNC1. Posicionar la innovación, la investigación aplicada y el desarrollo tecnológico en materia de ciberseguridad como habilitante para el desarrollo de la economía digital y tecnológica de Chile	Fortalecer de las capacidades de ciberseguridad en los organismos y empresas. Crear ente coordinador de la red de IAC del país para fortalecer las capacidades de ciberseguridad en los organismos y empresas del País. Crear Unidad Pública Gratuita de hacking ético. Crear Unidad certificadora de compliance con nivel de ciberseguridad en Software. Crear unidad certificadora de compliance en ciberseguridad para iot. Crear unidad certificadora de compliance en ciberseguridad para dispositivos médicos. Crear Dashboard Web de la operacionalización de la Política nacional vigente.	Nro de organismos apoyados Nro de hacking éticos realizados a Micro y pequeñas empresas Nro de organizaciones apoyadas por el ente que hayan formado capacidades de defensa Nro de software compliance nivel de ciberseguridad Nro de soluciones que incluyen iot compliance nivel de ciberseguridad Nro de dispositivos médicos con compliance nivel de ciberseguridad % de puntos abordados por la Política documentadas mostrando evidencia de su avance Nro de dispositivos Soluciones hackeados éticamente Nro de issues en registro nacional	Ente Regulador

OE	Iniciativas	KPI	Salidas Esperadas
	Crear unidad que sea contraparte Oxford para medir nivel de madurez de países.		
	Crear Dashboard Web de actividad de la red de centros de IAC en el País.		
	Crear unidad que sea contraparte NIST para la capacitación gratuita de estándares de ciberseguridad.		

Pilar 5: [Capacidades de Difusión/Colaboración Internacional]

→Programa: Foro Nacional de Ciberseguridad - Capítulo I+D+i: Fomentará la colaboración internacional y regional, estableciendo redes de trabajo y cooperación en ciberseguridad.

OE	Iniciativas	KPI	Salidas Esperadas
Establecer y fortalecer a Chile en el círculo de difusión/colaboración internacional de investigación en temas de ciberseguridad. Intercambio de experiencias con otros países en materia de ciberseguridad, con énfasis en la implementación y evaluación de estrategias y políticas.	Desarrollar un calendario de eventos/conferencias para potenciar la visualización de los resultados de las investigaciones. Instaurar canales formales de coordinación y colaboración internacional con las alianzas estratégicas. Coordinar los distintos canales de comunicación y colaboración entre las alianzas estratégicas.	Cantidad de acuerdos de cooperación (2) Sistema de gestión/ control de alianzas (3) Cantidad de eventos de difusión/visibilización en que se participa (4).	Normativa que defina el mecanismo en objetivo

OE	Iniciativas	KPI	Salidas Esperadas
Generar grupos de trabajo para Identificación y Promoción de distintas áreas de Investigación y colaboración Internacional	Participación del país en instancias multilaterales y globales apoyando de la misma forma procesos de consulta regional, subregional y multilateral en el área, particularmente en América Latina (al menos en materia de I+D en ciberseguridad). Grupo de trabajo interagencial para abordar temas internacionales relativos al ciberespacio. Definir un mecanismo (Foro o Forum) para unificar y representar a los investigadores en Chile en instancias internacionales, así como plataformas para producir la integración entre pares	Meses con eventos conferencias para diferentes estamentos Nro de suscritores a los canales/redes sociales para difusión Nro de participaciones globales de parte de la comunidad IAC Nro de instancias celebradas por el Foro Asistencia a las instancias celebradas por el Foro % Satisfacción de los participantes del foro.	Foro Nacional

→Acciones y Recomendaciones para el legislador:

1. Creación del Centro Nacional de Investigación en Ciberseguridad

Objetivo: Establecer un centro de referencia regional que coordine esfuerzos de investigación y desarrollo (I+D) en ciberseguridad, fomentando la colaboración entre la academia, el gobierno y el sector privado.

Acción Legislativa Urgente: Crear una ley que financie la creación de este centro, con un presupuesto asignado para infraestructura, contratación de personal especializado y alianzas internacionales. Este centro debe tener una estructura legal que permita la flexibilidad para atraer inversión extranjera y fomentar la colaboración público-privada.

2. Fomento de la Colaboración entre Academia, Industria y Gobierno

Objetivo: Establecer un ecosistema colaborativo entre sectores clave que acelere la innovación tecnológica y el desarrollo de soluciones de ciberseguridad.

Acción Legislativa Urgente: Promulgar una ley de incentivos fiscales y subsidios para proyectos de investigación conjuntos entre universidades, empresas tecnológicas y el gobierno. Esta legislación debe incluir fondos concursables específicos para proyectos de ciberseguridad y la creación de un marco legal que fomente la propiedad compartida de patentes y resultados.

3. Creación de un Laboratorio Nacional Distribuido para I+D en Ciberseguridad

Objetivo: Desarrollar una infraestructura compartida que permita a las instituciones de investigación y a las empresas probar y desarrollar nuevas tecnologías de ciberseguridad.

Acción Legislativa Urgente: Establecer un fondo estatal dedicado a la creación y mantenimiento de este laboratorio, con una legislación que permita a las instituciones públicas y privadas acceder a esta infraestructura. La ley debe definir mecanismos para asegurar que el laboratorio cuente con la tecnología más avanzada y que se fomente la participación de actores internacionales.

4. Marco Regulatorio para la Innovación en Ciberseguridad

Objetivo: Crear un marco legal que regule la investigación y el desarrollo en ciberseguridad, alineado con normativas internacionales, garantizando una innovación responsable y segura.

Acción Legislativa Urgente: Redactar y aprobar una ley que establezca un marco normativo claro para la investigación en ciberseguridad. Esta ley debe definir estándares mínimos de seguridad en el desarrollo de nuevas tecnologías, proteger la privacidad de los ciudadanos y garantizar la ética en la investigación tecnológica. Además, debe contemplar sanciones por incumplimiento y promover la adopción de mejores prácticas internacionales.

5. Desarrollo del Capital Humano Avanzado en Ciberseguridad

Objetivo: Aumentar el número de profesionales capacitados para realizar actividades de I+D en ciberseguridad mediante programas especializados en universidades y centros de formación técnica.

Acción Legislativa Urgente: Aprobar una ley que financie becas y programas educativos específicos para la formación en ciberseguridad. Esta ley debe incluir la creación de incentivos para que las empresas ofrezcan prácticas profesionales a estudiantes, así como subvenciones para la formación continua de profesionales en el sector público y privado.

6. Incentivos para la Innovación y el Emprendimiento en Ciberseguridad

Objetivo: Fomentar la creación de startups y el desarrollo de productos de base tecnológica en el área de ciberseguridad.

Acción Legislativa Urgente: Establecer un marco legal que ofrezca beneficios fiscales y apoyo financiero a las startups que trabajen en ciberseguridad. La legislación debe promover la inversión en investigación aplicada y establecer programas de financiamiento para el escalamiento de empresas tecnológicas emergentes en ciberseguridad.

7. Actualización de la Estrategia Nacional de Ciberseguridad

Objetivo: Revisar y actualizar periódicamente el Plan de Acción de la Política Nacional de Ciberseguridad así como la Estrategia Nacional de Ciberseguridad para adaptarla a las nuevas amenazas y tecnologías emergentes.

Acción Legislativa Urgente: Crear una ley que exija la revisión bianual de la Estrategia Nacional de Ciberseguridad, con la participación activa de actores públicos y privados. Esta ley debe incluir mecanismos de consulta con la sociedad civil y expertos internacionales para asegurar que las políticas de ciberseguridad estén alineadas con los estándares internacionales.

→ Resumen de acciones prioritarias.

Acción Prioritaria	**Iniciativa**	**Descripción**	**Responsables**	**Plazo estimado**
1.Fortalecimiento del Ecosistema de Investigación y Desarrollo (I+D)	Programa de Inversión Público-Privada para I+D+i	Chile necesita aumentar los fondos destinados específicamente a la investigación en ciberseguridad. Esto puede incluir la creación de incentivos fiscales para empresas que inviertan en I+D, o financiamiento estatal para proyectos de innovación, o la estimulación de la asociación virtuosa del sector público-privado y académico.		
	Desarrollo de Centros de Innovación	Es necesario establecer centros de excelencia o institutos de investigación que colaboren con la industria, el gobierno y la academia. Estos centros serían responsables de la creación de nuevas tecnologías y soluciones ante las amenazas emergentes en		

		ciberseguridad.		
	Formación, Retención y Captación de Capital Humano Avanzado en Ciberseguridad	Para alcanzar un nivel de madurez en investigación e innovación, es necesario no solo aumentar la oferta de programas educativos en pregrado y posgrado, sino también especializar estos programas en temas como inteligencia artificial aplicada a la ciberseguridad, análisis de riesgos emergentes y desarrollo de tecnologías disruptivas.		
2. Creación y Fortalecimiento de Alianzas Público-Privadas y Colaboración Internacional	Aumentar la participación en consorcios internacionales	Chile debe integrarse activamente en redes de investigación regionales e internacionales, como la Unión Europea y otros foros especializados en ciberseguridad. La participación en proyectos colaborativos permitiría aprovechar mejores prácticas globales y recursos tecnológicos avanzados.		

→ Resumen de acciones prioritarias.

	Fomentar la colaboración público-privada	La investigación en ciberseguridad requiere la colaboración entre empresas privadas, universidades y el Estado. Iniciativas como laboratorios conjuntos o consorcios que combinen recursos y conocimientos permitirían avanzar más rápidamente.		
3. Formación de Investigadores en Ciberseguridad		Para mantener una base sólida de profesionales y académicos que impulsen la investigación en ciberseguridad, Chile debe generar incentivos tanto para la formación, como para que los talentos formados en el país no migren a otros mercados más avanzados. Crear un entorno atractivo para la innovación local es clave.		

4. Contribución a la Cultura de Investigación e Innovación en Ciberseguridad	Indicadores Clave de desempeño (KPI)	Chile debe establecer indicadores claros y medibles para evaluar el impacto de sus iniciativas en I+D en ciberseguridad. Esto puede incluir la cantidad de patentes, publicaciones, o colaboraciones a nivel nacional e internacionales que se generen a partir de los proyectos de investigación.		
	Evaluación continua de amenazas emergentes	Los marcos legales y las estrategias nacionales deben ser revisados y actualizados regularmente en función de los nuevos riesgos y desafíos que surjan en el ámbito digital.		
	Fomento de la Ciber Higiene y la Innovación desde la Base	Es necesario hacer hincapié en la necesidad de trabajar en la alfabetización digital y la ciberhigiene. Un entorno donde la seguridad es una prioridad desde los niveles más básicos impulsa también una cultura de innovación, ya que los profesionales se sienten respaldados para experimentar con nuevas soluciones.		
	Construcción de Comunidades de Interés	Deben crearse plataformas que permitan la participación de investigadores, empresas y reguladores en el desarrollo de soluciones innovadoras, creando un ecosistema donde la innovación fluya naturalmente.		

→ Conclusiones

El análisis del Foro D3.4 sobre el camino hacia la madurez en investigación e innovación en ciberseguridad para Chile ha identificado una serie de recomendaciones clave para impulsar el desarrollo del sector en el país. Estas recomendaciones se centran en fortalecer el ecosistema de investigación y desarrollo, fomentar la colaboración entre los actores clave, y crear un marco regulatorio favorable para la innovación.

Las principales conclusiones y recomendaciones son las siguientes:

- **Creación de un centro de referencia nacional:** Se propone la creación de un Centro Nacional de Investigación en Ciberseguridad que coordine los esfuerzos de I+D, fomente la colaboración y atraiga inversión extranjera.

- **Fomento de la colaboración público-privada:** Se recomienda establecer un ecosistema colaborativo entre academia, industria y gobierno a través de incentivos fiscales y subsidios para proyectos conjuntos.

- **Desarrollo de infraestructura compartida:** Se propone la creación de un Laboratorio Nacional Distribuido para I+D en Ciberseguridad que permita a las instituciones y empresas probar y desarrollar nuevas tecnologías.

- **Marco regulatorio claro:** Se requiere un marco legal que regule la investigación y el desarrollo en ciberseguridad, garantizando una innovación responsable y segura.

- **Desarrollo de capital humano avanzado:** Se deben aumentar los programas de formación en ciberseguridad y ofrecer incentivos para que las empresas ofrezcan prácticas profesionales.

- **Incentivos para la innovación y el emprendimiento:** Se deben establecer beneficios fiscales y apoyo financiero para las startups que trabajen en ciberseguridad.

- **Actualización periódica de la estrategia nacional:** Se debe revisar y actualizar la Estrategia Nacional de Ciberseguridad para adaptarla a las nuevas amenazas y tecnologías emergentes.

En resumen, el fortalecimiento de la investigación e innovación en ciberseguridad en Chile requiere de una acción coordinada entre el gobierno, la academia y el sector privado. La implementación de estas recomendaciones permitirá a Chile posicionarse como un referente regional en ciberseguridad y contribuir al desarrollo de soluciones innovadoras para enfrentar los desafíos actuales y futuros en este ámbito.

→ Glosario de Términos

1. Ciberseguridad: Conjunto de prácticas, tecnologías y procesos diseñados para proteger redes, dispositivos, programas y datos de ataques, daños o acceso no autorizado.

2. Capital Humano Avanzado: Acumulación de conocimientos, habilidades y competencias especializadas que poseen individuos con educación superior, formación técnica avanzada y experiencia profesional significativa, permitiéndoles contribuir de manera innovadora y eficiente en sectores complejos y de alta tecnología.

3. I+D (Investigación y Desarrollo): Actividades empresariales o académicas que buscan crear nuevos conocimientos o desarrollar tecnologías innovadoras.

4. Ciberhigiene: Prácticas rutinarias que los usuarios y las organizaciones deben seguir para mantener sistemas y datos seguros, como actualizar software, usar contraseñas seguras y evitar enlaces sospechosos.

5. TRL (Technology Readiness Level): Escala que mide el nivel de madurez de una tecnología en desarrollo, desde la investigación básica (nivel 1) hasta su uso en el mercado (nivel 9).

6. KPI (Key Performance Indicators o Indicadores Clave de Desempeño): Métricas que se utilizan para medir el éxito o el progreso de una iniciativa o proyecto en ciberseguridad.

7. Centro Nacional de Investigación en Ciberseguridad: Institución dedicada a coordinar y promover la investigación y desarrollo en ciberseguridad, tanto a nivel nacional como internacional.

8. Laboratorio Nacional Distribuido para I+D en Ciberseguridad: Infraestructura que permite el desarrollo y la prueba de tecnologías de ciberseguridad por parte de diferentes actores (academia, industria, gobierno) en distintas localizaciones.

9. Colaboración Público-Privada: Asociación entre el sector público (gobierno) y privado (empresas) para llevar a cabo proyectos conjuntos que beneficien a ambos sectores, especialmente en áreas de innovación y desarrollo tecnológico.

10. Marco Regulatorio: Conjunto de leyes y normativas que establecen los parámetros dentro de los cuales deben realizarse actividades específicas, como la investigación en ciberseguridad.

11. Innovación: Proceso de creación de nuevas ideas, productos o servicios que aportan mejoras significativas a un campo o industria, en este caso, el ámbito de la ciberseguridad.

12. Startups: Empresas emergentes que desarrollan productos o servicios innovadores, a menudo con un alto componente tecnológico.

13. Estrategia Nacional de Ciberseguridad: Plan del gobierno que establece los objetivos, políticas y acciones a seguir para proteger la infraestructura digital del país y responder a las amenazas cibernéticas.

14. Consorcios Internacionales de I+D: Alianzas entre diferentes países, empresas o instituciones que colaboran en proyectos de investigación y desarrollo de tecnologías, compartiendo conocimientos y recursos.

15. Infraestructura Crítica: Sistemas y activos esenciales para el funcionamiento de una sociedad y su economía, tales como redes de energía, agua, telecomunicaciones y transporte, que requieren protección frente a ataques cibernéticos.

16. Amenazas Cibernéticas: Cualquier actividad maliciosa que busque comprometer la seguridad, disponibilidad o integridad de los sistemas de información o redes, como el malware, phishing, ataques de denegación de servicio (DDoS), etc.

17. Privacidad por Diseño: Enfoque de desarrollo de tecnologías y sistemas que integran la protección de la privacidad y los datos personales desde las primeras fases de diseño y no como un añadido posterior.

18. Redes de Colaboración en Investigación: Grupos o asociaciones de investigadores y organizaciones que trabajan juntos para desarrollar conocimiento y tecnologías en un área específica, como la ciberseguridad.

19. Alfabetización Digital: Conjunto de conocimientos y habilidades necesarias para utilizar tecnologías digitales de manera segura, eficiente y responsable.

→ REFERENCIAS

1. Biblioteca del Congreso Nacional de Chile. (n.d.). Construyendo la Ciberseguridad en Chile. https://obtienearchivo.bcn.cl/obtienearchivo?id=documentos/10221.1/89176/3/Construyendo_la_Ciberseguridad_en_Chile.pdf

2. Centro Criptológico Nacional. (2023). Foro Nacional de Ciberseguridad. Gobierno de España. https://www.ccn.cni.es/index.php/es/menu-ccn-es/foro-nacional-de-ciberseguridad

3. Centro de Innovación UC & Microsoft Chile. (2022). Hoja de Ruta de Ciberseguridad. Centro de Innovación UC. Retrieved from https://centrodeinnovacion.uc.cl/hoja-de-ruta-de-ciberseguridad/

4. Departamento de Seguridad Nacional. (2023). Foro Nacional de Ciberseguridad - Motor de la colaboración público-privada. Gobierno de España. https://www.dsn.gob.es/es/documento/foro-nacional-ciberseguridad-motor-colaboraci%C3%B3n-p%C3%BAblico-privada

5. Foro Nacional de Ciberseguridad de Chile. (2020). Reporte de ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe. https://www.forociber.cl/foro/site/docs/20240322/20240322150520/reporte_ciberseguridad_2020_riesgos_avances_y_el_camino_a_seguir_en_america_latina_y_el_caribe.pdf

6. Foro Nacional de Ciberseguridad. (2023). Grupos de trabajo. https://foronacionalciberseguridad.es/grupos-de-trabajo

7. Global Cyber Security Capacity Centre. (2021). Cybersecurity Capacity Maturity Model (CMM) for Nations. University of Oxford. https://gcscc.ox.ac.uk/the-cmm

8. Gómez, J., & López, M. (2020). Título del artículo. Perspectivas en Educación, 20(3), 123-135. Recuperado de https://www.scielo.br/j/pee/a/YyZgKBY9JLVXnCDKMNc7nqc/?lang=es&f

9. Ministerio de Ciencia, Tecnología, Conocimiento e Innovación. (2021). Política Nacional de Inteligencia Artificial. Gobierno de Chile. https://www.minciencia.gob.cl/areas/inteligencia-artificial/politica-nacional-de-inteligencia-artificial/

10. Ministerio del Interior y Seguridad Pública. (2023). Política Nacional de Ciberseguridad 2023-2028. Gobierno de Chile. https://ciberseguridad.gob.cl/pncs-2023-2028/

11. National Institute of Standards and Technology (NIST). (n.d.). Workplace skills and NICE Framework. NIST. Recuperado de https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workplace-skills-and-nice-framework 1

2. Órdenes, X., Roberts, R., Rojas, F., & Rojas, P. (2023). Estrategia de transformación digital: Chile Digital 2035. Comisión Económica para América Latina y el Caribe (CEPAL). https://www.cepal.org/es/publicaciones/49067-estrategia-transformacion-digital-chile-digital-2035

13. Pacheco, F. (n.d.). Educación en ciberseguridad mediante estrategias de gamificación. ResearchGate. https://www.researchgate.net/publication/385096975.

14. Pérez, J., & López, M. (2020). Uso de estrategias tecnológicas en la educación. Educación y Tecnología, 15(3), 45-60. Recuperado de https://www.redalyc.org/journal/614/61458265007/61458265007.pdf.

15. Zepeda-Hurtado, M. E., Cardoso-Espinosa, E. O., & Rey-Benguría, C. (2019). El desarrollo de habilidades blandas en la formación de ingenieros. Científica, 23(1), 61-67. Recuperado de: https://www.redalyc.org/journal/614/61458265007/61458265007.pdf

DIMENSIÓN 4:

Marcos Legales y Regulatorios

Moderador:
Juan Pablo González

Agradecimientos

Un especial agradecimiento a quienes participaron en las discusiones de esta Dimensión:

- **Jessica Narváez.**
- **Matías Rojo.**
- **Roberto Poblete.**
- **Leonardo Fuentes.**
- **uan Hernández.**
- **Carolina Sancho.**

Como al equipo redactor del presente Informe (primera versión):

- **Sebastián Izquierdo.**
- **Álvaro Rodrigo Cayul.**
- **Josefa Zamorano.**
- **Héctor Moyano.**
- **Luis Pando Torres.**

Equipo revisor y editor (versión final).

- Revisores: **Sergio Miranda y Catherine Narváez.**
- Editor y Representante de la Dimensión: **Juan Pablo González.**

→ 1. PRESENTACIÓN DE LA DIMENSIÓN Nº 4

La Dimensión N° 4 del Foro Nacional tiene como ejes principales los marcos legales y regulatorios de ciberseguridad en Chile.

Esta dimensión busca examinar la capacidad del Gobierno para diseñar y promulgar legislación nacional que se relacionen directa e indirectamente con la ciberseguridad, con un énfasis particular en los temas de los requisitos regulatorios para la misma, protección de datos personales, legislación relacionada con los delitos informáticos, junto con las demás normativas relacionadas como también. la capacidad para hacer cumplir la normativa legal vigente, formular propuestas para homologar los criterios de evaluación, proponer controles para medir la aplicación de la ley, junto a la coordinación con la institucionalidad existente, incluyendo los órganos reguladores y los tribunales de justicia son ámbitos que deben ser abordados para integrar todo este ecosistema normativo a nuestro ordenamiento jurídico nacional. Además, esta dimensión observa los marcos de cooperación formales e informales para combatir el cibercrimen.

Este dominio se dividió en:

4.1 Disposiciones legales y regulatorias: este factor aborda diversas leyes y provisiones de regulación a la ciberseguridad, incluidos los requisitos legales y regulatorios, legislación sustantiva y procesal sobre ciberdelincuencia e impacto, y evaluación sobre los derechos humanos.

4.2. Marcos legislativos relacionados: este factor aborda los marcos legislativos relacionados a la ciberseguridad, incluida la protección de datos, protección de niños, niñas y adolescentes en el uso de tecnología, protección del consumidor y la propiedad intelectual.

4.3. Capacidad, habilidad legal y regulatoria: este factor estudia la capacidad de aplicar la ley para investigar los delitos informáticos, la capacidad del Ministerio Público para presentar casos de ciberdelincuencia, pruebas electrónicas y custodia de ellas, junto con la capacidad de los tribunales de justicia para presidir casos de ciberdelincuencia y que involucren evidencia electrónica. Finalmente, este factor revisa la existencia de organismos reguladores intersectoriales para supervisar el cumplimiento de normativas específicas de ciberseguridad.

4.4. Marcos de cooperación formal e informal para combatir el cibercrimen: este factor aborda la existencia y función de los mecanismos formales e informales que permitan la cooperación entre actores nacionales y transfronterizos para disuadir y combatir el cibercrimen.

El objetivo principal fue analizar y evaluar las normativas existentes y los desafíos pendientes para desarrollar una hoja de ruta que impulse la madurez cibernética nacional. Este trabajo se realizó bajo el enfoque del **Modelo de Madurez de Ciber Capacidades para las Naciones (CMM)** de la Universidad de Oxford, evaluando temas como regulación, cooperación interinstitucional y la capacidad del Estado para implementar las normativas.

Por decisión de los integrantes de la Dimensión, se optó por agrupar los cuatros sub-factores dentro de la Dimensión “Marcos Legislativos y Regulatorios”, donde se abordaron las leyes que se vinculan directamente con ciberseguridad, como aquellas que están relacionadas y los desafíos que se identificaron por los integrantes del equipo de trabajo.

El presente informe incluye un análisis detallado de varias leyes claves, como lo son la Ley Marco de Ciberseguridad, la Ley de Protección de Datos Personales y la Ley de Delitos Informáticos, además de otras normativas asociadas. En este análisis, se identificaron tanto fortalezas como desafíos en su implementación, proponiendo, además, para mejorar su eficacia según la perspectiva de los miembros del equipo que trabajó en esta área.

→ 2. ANTECEDENTES

→ A. El avance normativo de Chile respecto a otros países de la región

Chile ha experimentado un avance significativo en la incorporación de un marco normativo para las tecnologías de la información (TI), impulsado por la necesidad de adaptarse a la rápida evolución digital y fomentar la competitividad en la región. Nuestro país ha desarrollado normas y un marco regulatorio sólido que abarca diversos aspectos, como la ciberseguridad, la protección de datos personales y servicios financieros basados en tecnología y comercio electrónico. Estas iniciativas han sido fundamentales para generar confianza en el entorno digital y promover la inversión en tecnologías de la información.

Comparado con otros países de la región, Chile se ha posiciona favorablemente en términos de competitividad digital. Según el Índice de Desarrollo de las TIC de la Unión Internacional de Telecomunicaciones (UIT), Chile ocupa el primer lugar en América Latina y el Caribe. Este índice evalúa diversos aspectos como el acceso, el uso, la asequibilidad, la calidad y las habilidades relacionadas con las TIC. El marco regulatorio chileno, junto con las inversiones en infraestructura y la promoción de la innovación, han contribuido a este liderazgo regional. Este liderazgo se debe no solo a un marco regulatorio sólido, sino también a las importantes inversiones en infraestructura digital, como el despliegue de redes de fibra óptica y la expansión de la cobertura de internet. Además, Chile ha implementado programas para promover la alfabetización digital y el desarrollo de habilidades TIC en la población, lo que ha contribuido a un mayor uso y aprovechamiento de las tecnologías. Continuando con esta estrategia, Chile se ubica en una posición destacada en el Índice Global de Ciberseguridad (GCI) del ITU, lo que refleja su compromiso con la seguridad en el entorno digital.

Chile destaca en la región por su posición favorable en el ámbito tecnológico. El país ha desarrollado una infraestructura tecnológica sólida y cuenta con profesionales cualificados en tecnologías de la información. Nuestro país ha logrado establecer una infraestructura tecnológica robusta, así como una fuerza laboral capacitada en áreas relacionadas con las tecnologías de la información. Además, el gobierno ha implementado políticas y programas de apoyo a la innovación y al emprendimiento digital, lo que ha impulsado el desarrollo de un ecosistema tecnológico dinámico y competitivo.

Por otra parte, según el Comité Interamericano Contra el Terrorismo (CICTE), órgano dependiente de la Organización de los Estados Americanos (OEA) y que ha apoyado en el desarrollo de estrategias de ciberseguridad para los Estados Miembros, en la región, ha habido un incremento en la generación de normas y marco regulatorio en torno a la ciberseguridad, protección de datos personales, inteligencia artificial y otras normas asociadas al mundo de las tecnologías de la información (TI). Para evaluar este avance, ha fijado conceptos relevantes, tales como: Gobernanza, resiliencia, desarrollo de capacidades en la ciudadanía, coordinación y cooperación nacional e internacional, desarrollo de un marco normativo, investigación y desarrollo, además del nivel de observancia o adhesión a tratados internacionales, como el Convenio de Budapest.

En 2024, Chile se destacó junto a Argentina en el cumplimiento de estos conceptos, incluido ser miembro y adherente del Segundo Protocolo del Convenio de Budapest, seguido de Uruguay, que cumple con la mayoría de los aspectos evaluados y que a la fecha cuenta con el estatus de Observador del Convenio. Otros países que han ido avanzando en el cumplimiento de los aspectos evaluados por CICTE-OEA, han sido Costa Rica, Ecuador y República Dominicana y, si bien estos dos últimos países tienen puntos relevantes a cumplir, ya han establecido estrategias específicas referentes a la ciberdelincuencia, ciberdefensa y ciberterrorismo, diferenciándose de otras naciones donde recién han comenzado estas iniciativas.

Sin embargo, los avances también representan desafíos, dentro los cuales destacan la falta de una madurez cultural de la sociedad en el conocimiento de materias de tecnología y ciberseguridad, la falta de especialización técnica y la brecha digital, no sólo de género, sino también para las personas pertenecientes al grupo etario de adultos mayores y los niños, niñas y adolescentes que se exponen por el poco conocimiento al mundo digital, sin medir las consecuencias o los fines ulteriores que otros agentes pueden llevar a cabo con su información personal.

→ B. Metodología de Trabajo

El trabajo de la Dimensión N° 4, posterior a una discusión de quienes lo lideran y aprobación de los integrantes del mismo, siguió una metodología estructurada basada en:

a. Análisis regulatorio.

1. Análisis normativo: revisión de leyes vigentes relevantes para la ciberseguridad como la Ley Marco de Ciberseguridad, Ley de Protección de Datos Personales, Ley de Delitos Informáticos, además de otras leyes relacionadas, a saber: Ley de Transformación Digital, Ley de Infraestructura Crítica y Ley que establece Internet como servicio público.

2. Encuestas y consultas: los participantes respondieron preguntas sobre desafíos, implementación y propuestas para cada normativa.

3. Debate guiado: se abrieron hilos de discusión organizados por temáticas específicas, facilitando el intercambio de ideas y experiencias.

4. Evaluación con el modelo CMM: cada normativa se evaluó respecto a su contribución al desarrollo de capacidades cibernéticas nacionales.

b. Discusión - Hallazgos Generales

Entre los principales hallazgos obtenidos del proceso de revisión de las normativas, se pueden observar los siguientes aspectos.

1. Diversidad de niveles de madurez en las organizaciones: las instituciones privadas y los organismos públicos enfrentan grandes diferencias en su capacidad para cumplir con las normativas, especialmente, aquellas que contienen una serie de requisitos que implican ya no sólo un enfoque de cumplimiento a través de medidas organizativas, sino también, cambios en sus procesos, estructuras y personal.

Desafíos en la implementación: las organizaciones públicas y privadas, desde la experiencia del equipo de trabajo, hay falta de recursos económicos, personal capacitado y directrices claras; lo que fue un tema que surgió reiteradamente en las discusiones de cada uno de los puntos.

Cultura: la necesidad de una cultura organizacional que priorice no sólo la seguridad cibernética sino de las otras normativas que permiten apoyar la ciberseguridad, como la protección de datos personales u otras, es clave y fundamental.

c. Resultados de la Discusión

Los principales resultados de las discusiones dirigidas fueron:

• Identificación de puntos críticos en la implementación de normativas clave.

• Propuestas para fortalecer la coordinación interinstitucional, entre todos los actores que conforman el ecosistema de gobernanza de la ciberseguridad.

• Estrategias para apoyar a PyMEs y otros sectores vulnerables en su transición hacia el cumplimiento regulatorio y permitirles acceder de manera equitativa a los beneficios que esto conlleva.

→ 3. ANÁLISIS POR TEMÁTICA

→ A. Ley Marco de Ciberseguridad (Ley Nº 21.663)

La Ley Marco Nº 21.663, crea la Agencia Nacional de Ciberseguridad (ANCI), además de generar una gobernanza en la materia, a través del reconocimiento normativo del Comité Interministerial de Ciberseguridad, y la creación de un Consejo Multisectorial de Ciberseguridad que reúna a la academia y el sector privado en la discusión de la ciberseguridad.

Esta norma, establece un listado no taxativo de instituciones públicas y privadas que proveen servicios esenciales, y reconoce a **Operadores de Importancia Vital (OIV).** Para ambos sujetos obligados, establece una serie de deberes generales y específicos, entre los que se destaca la necesidad de adoptar un enfoque integral en cuanto a la gestión de los incidentes de ciberseguridad y brechas de datos, y especialmente, en el caso de aquellos OIV el establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI). Finalmente, ambos tienen la obligación de reportar incidentes a la ANCI, canalizadas a través del CSIRT Nacional.

Establece una serie de multas en caso de infracción cuyo máximo en el caso de los servicios esenciales es de 20.000 UTM y, en el caso de OIV son 40.000 UTM. Finalmente, con fecha del 24 de diciembre de 2024, se publicó el decreto con fuerza de ley mediante el cual la ANCI comenzó sus funciones a contar del 1 de enero de 2025, junto con determinar la entrada en vigor de las disposiciones de la Ley Nº 21.663 relativo a los operadores de importancia vital, notificación de incidentes y el sistema sancionatorio a contar del 1 de marzo de 2025.

De las discusiones sostenidas por los integrantes de la Dimensión se puede destacar:

Fortalezas:

• La Ley Marco de Ciberseguridad se establece como un instrumento regulatorio robusto que incluye definiciones claras sobre servicios esenciales.

• Creación de una entidad especializada con facultades fiscalizadoras y sancionatorias como la ANCI.

• Ser una normativa pionera en la región tomando como referente el enfoque de la Directiva Europea NIS2.

Desafíos:

• Comenzar el funcionamiento de la ANCI durante el 2025[2]

• Falta de reglamentos secundarios para operativizar la ley[3]

• Necesidad de establecer criterios homogéneos para los reportes de incidentes de impacto significativo.

• Elaboración del primer listado de OIV y su proceso de adherencia.

• Desafíos en la fiscalización de OIV y servicios esenciales.

• Implementar un sistema de evaluación con indicadores clave de desempeño (KPIs) para medir el impacto efectivo de la Ley y la eficacia operativa de la Agencia, como, por ejemplo, la reducción cuantificable de incidentes cibernéticos.

Propuestas:

• Establecer, en colaboración con el Ministerio de Economía, directrices específicas para PyMEs que faciliten su transformación digital, optimicen sus procesos estratégicos y fortalezcan sus prácticas de seguridad digital, contemplando incentivos tributarios y mecanismos de apoyo financiero para la implementación efectiva de la normativa.

• Implementar campañas de concientización y ciberhigiene en colaboración con el sector académico para la sociedad.

[2] A la fecha de la discusión del Foro estaba pendiente este desafío. No obstante, , con fecha 24 de diciembre del 2024, se publicó el DFL Nº1, de la Ley Nº 21.663, que establece que las actividades de la Agencia Nacional de Ciberseguridad inician con fecha 1º de enero del 2025.

[3] A la fecha en que se produjeron las discusiones estaba pendiente la publicación de los Reglamentos de la Ley Nº 21.663. Hoy en día, se encuentran publicados los reglamentos: Funcionamiento del Comité Interministerial de Ciberseguridad (Decreto Nº 275); Establece normas para el funcionamiento del Consejo Multisectorial sobre Ciberseguridad (Decreto Nº 276), Reporte de incidentes de Ciberseguridad de la Ley Nº 21.663 (Decreto Nº 295).

→ B. Ley de Protección de Datos Personales (Ley Nº 19.628) y su reforma (Ley N° 21.719)

La Ley Nº 19.628 sobre protección a la vida privada que data del año 1999, ha sido objeto de un proceso de una actualización profunda y acorde a nuestro tiempos mediante la publicación de la Ley Nº 21.719 que crea la Agencia de Protección de Datos Personales. Dicho cuerpo legal comenzará su entrada en vigor a contar del 1º de diciembre de 2026, lo que obligará a las organizaciones públicas y privadas a adaptar y mejorar sus procesos y estándares a las nuevas exigencias normativas inspiradas principalmente en el Reglamento General de Protección de Datos de la Unión Europea (RGPD).

Entre los elementos destacables de la normativa reformada se encuentran: el establecimiento de principios para el tratamiento de datos personales; obligaciones específicas para responsables y encargados del tratamiento; un régimen especial sobre transferencias internacionales de datos personales; la promoción de la autorregulación mediante la creación voluntaria de un Modelo de Prevención de Infracciones (que incluye la designación de un Delegado de Protección de Datos Personales); y un sistema de sanciones por incumplimiento que puede alcanzar hasta 20.000 UTM. En caso de reincidencia, para empresas que no califican como pequeñas o medianas, las multas pueden ascender al 2% o 4% de las ventas anuales de productos o servicios en territorio nacional. Cabe señalar que la ley establece un tratamiento diferenciado para pequeñas empresas, tanto en materia de sanciones como en estándares mínimos de cumplimiento.

De las discusiones sostenidas por los integrantes de la Dimensión se puede destacar:

Fortalezas:

- Inspiración en la normativa internacional más actualizada, que permitirá tener un enfoque global en materia de protección de datos personales, en cuanto a principios, ejercicio de derechos, transferencia internacional de datos, entre otros.

- Creación de la Agencia Nacional de Protección de Datos, especializada que permita la existencia de sanciones frente al incumplimiento de la normativa, a través de un procedimiento sancionatorio que establece multas a las organizaciones públicas y privadas que no den un cumplimiento ajustado a la Ley.

Desafíos:

- Implementación coordinada con la Ley Marco de Ciberseguridad (Ley Nº 21.663).

- Coordinar la aplicación eficaz del régimen sancionatorio entre ambas Agencias para prevenir la duplicidad de sanciones y garantizar la proporcionalidad en su imposición.

- Capacitación de profesionales en protección de datos para aquellos que asuman como Delegado de Protección de Datos Personales (DPD/DPO).

Propuestas:

- Integrar ambas normativas en sistemas de cumplimiento integrales dentro de las organizaciones.

• Definir claramente los roles y responsabilidades de las agencias regulatorias.

→ C. Ley de Delitos Informáticos (Ley Nº 21.459) y su relación con la Ley de Delitos Económicos (Ley Nº 21.595)

La Ley Nº 21.459 establece normas sobre delitos informáticos adecuando la normativa existente al Convenio de Budapest, por lo que deroga la Ley Nº 19.223, que se encargaba de tipificar algunas figuras penales relativas a la informática y, además, modifica otros cuerpos legales relacionados. Esta norma fue promulgada en junio de 2022, incluyendo una serie de conductas como delitos informáticos, además de fijar las reglas procesales para su persecución.

Otro de los cambios que conlleva la aplicación de esta norma, es que también se integran los delitos informáticos como aquellos que pueden generar la responsabilidad penal de las personas jurídicas, de acuerdo con lo establecido en la Ley Nº 20.393. Del mismo modo, los delitos informáticos son también considerados delitos económicos de segunda categoría, según lo establece el art. 2° de la Ley Nº 21.595 (en adelante, Ley de Delitos Económicos). Esto implica, que cuando un delito informático sea cometido en ejercicio de un cargo, función o posición en una empresa, en su beneficio o no, habrá responsabilidad penal corporativa también para aquella organización a la que pertenezca el autor del delito, aplicándose, por tanto, el estatuto reforzado de la Ley de Delitos Económicos, que conlleva sanciones más gravosas y una determinación de la pena mucho más estricta que el régimen general.

La Ley de Delitos Informáticos establece ocho figuras típicas, a saber: (i) ataque a la integridad de un sistema informático; (ii) acceso ilícito; (iii) interceptación ilícita; (iv) ataque a la integridad de los datos informáticos; (v) falsificación informática; (vi) receptación de datos informáticos; (vii) fraude informático; y (viii) abuso de los dispositivos. Cada una de ellas se refiere a la afectación de un bien jurídico en particular, en algunos casos, a los datos o información, en otros, al sistema informático como bien material, y en otros, a la seguridad informática como un valor superior. Por otro lado, algunos de estos delitos son delitos de mera actividad, por ejemplo, el acceso ilícito, la interceptación ilícita o la falsificación informática, otros, en cambio, de resultado, como es el caso del ataque a la integridad de los datos o sistemas informáticos o el fraude informáticos. Por último, vale la pena mencionar que para la configuración típica de estos delitos se requiere dolo, el que, sin perjuicio, puede ser un dolo eventual.

La Ley de Delitos Informáticos también establece dos circunstancias agravantes, y ninguna atenuante -este último cambio se introdujo con la ley Nº 21.694 de septiembre de 2024, que eliminó el artículo 9° que establecía la cooperación eficaz como atenuante especial-.

Las circunstancias agravantes se disponen en el artículo 10° y se refieren a:

1) Cometer el delito abusando de una posición de confianza en la administración del sistema informático o como custodio de los datos que son afectados.

2) Abuso de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores.

Para cualquier caso, se establece que, si la comisión del delito afectase o interrumpiera la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos electorales regulados en la ley Nº 18.700, orgánica constitucional sobre votaciones populares y escrutinios, en cuyo caso la pena se aumentará en un grado.

Por último, cabe señalar que la Ley Nº 21.663, Ley Marco de Ciberseguridad, también conlleva reformas en la Ley de Delitos Informáticos en lo que dice relación con la posibilidad de realizar pruebas de vulnerabilidad en sistemas informáticos, para lo cual exigirá que quienes se dediquen a este tipo de actividades estén debidamente inscritos en un registro especial que tendrá para tales efectos la ANCI y cumplan con las demás condiciones que indica el propio artículo 2°, referido al acceso ilícito.

En cuanto a las normas procesales, cabe destacar, que además de las reglas generales sobre legitimación activa, la investigación de los delitos informáticos puede iniciarse por querella del Ministerio del Interior y Seguridad Pública, o de los secretarios o secretarias regionales ministeriales de seguridad pública, cuando estas interrumpan el normal funcionamiento de un servicio de utilidad pública.

Asimismo, contempla medidas de investigación intrusivas, como lo son la interceptación de comunicaciones y el actuar de los agentes encubiertos. También, se establece el comiso de los instrumentos de los delitos, sus efectos y utilidades o a una suma de dinero equivalente.

De las discusiones sostenidas por los integrantes de la Dimensión se puede destacar:

Fortalezas:

- Se recomienda una aproximación de modernización de la normativa para adaptarse a delitos cibernéticos emergentes.

- Armonización con estándares internacionales, ej. Protocolos Adicionales del Convenio de Budapest.

Desafíos:

- Obsolescencia potencial frente a la rápida evolución tecnológica considerando que el Convenio de Budapest data del año 2001.

- Falta de revisiones periódicas a la normativa.

- Definiciones altamente técnicas que complejizan su comprensión por parte de los entes de persecución penal, lo cual dificulta también su efectiva persecución.

Propuestas:

- Se recomienda establecer revisiones legislativas periódicas para evaluar su efectividad.

• Implementar prácticas internacionales en detección y sanción de ciberdelitos.

• Capacitación y especialización de Carabineros de Chile y Policía de Investigaciones de Chile en materia de investigación de delitos informáticos.

→ D. Otras Normativas Analizadas

i. Ley de Infraestructuras Críticas (Ley Nº 21.542)

La Ley N° 21.542 modificó la Constitución Política de la República de Chile, incorporando una nueva atribución del Presidente de la República que le permite disponer que las Fuerzas Armadas asuman la protección de la infraestructura crítica nacional cuando está enfrente peligro grave o inminente. La normativa establece con precisión el concepto de infraestructura crítica y regula los mecanismos operativos mediante los cuales las Fuerzas Armadas ejercerán estas funciones de resguardo. Adicionalmente, esta ley amplía las competencias de las Fuerzas Armadas para incluir la vigilancia y protección de determinadas áreas en zonas fronterizas del territorio nacional.

La Ley Nº 21.542 puede impactar indirectamente a la ciberseguridad y protección de datos personales al fortalecer la seguridad física y digital de sistemas considerados esenciales. No obstante, en la práctica esta normativa no aborda directamente la Ley Marco de Ciberseguridad y Ley de Protección de Datos Personales, por lo que no se ha podido profundizar en experiencias que den cuenta del desempeño de esta regulación.

De las discusiones sostenidas por los integrantes de la Dimensión se puede destacar:

Fortalezas:

• Definición de infraestructura crítica e importancia del resguardo para el país se plasman en una modificación constitucional.

Desafíos:

• Coordinación limitada entre reguladores y operadores de infraestructura crítica.

• Nula aplicación de la normativa en materias de infraestructura crítica de seguridad de la información, siendo su principal enfoque en el resguardo de zonas fronterizas.

• Falta de capacitación y recursos para implementar estándares internacionales como NERC-CIP, 5G, y otras normativas que puedan ser impuestas por el regulador.

Propuestas:

• Utilizar un marco de referencia para facilitar la adopción de métricas estandarizadas para evaluar cumplimiento y madurez en la protección de infraestructuras críticas.

• Desarrollar planes de formación para el personal de las Fuerzas Armadas en materia de infraestructura crítica de seguridad de la información, que serán empleados en su debido resguardo a solicitud del Presidente de la República.

ii. Ley de Transformación Digital (Ley Nº 21.180)

La ley N° 21.180 tiene como principal objetivo modernizar la labor de la administración del Estado, en especial el desarrollo de sus procesos administrativos y su relacionamiento con la ciudadanía en general. En el desempeño de dicho cometido, la ley ha fijado su proceso de implementación al 31 de diciembre del año 2027, debiendo el sector público actualizarse y adoptar sus procedimientos para dar cumplimiento a los cometidos de esta normativa.

El proceso de transformación digital necesita la incorporación de nuevas tecnologías, las que traen consigo riesgos para los miembros de la administración del Estado que operarán estos sistemas o plataformas, como a la ciudadanía en general, cuya información personal será tramitada a través de mecanismos electrónicos.

• Desde la perspectiva de la ciberseguridad, los aspectos fundamentales que deben considerarse son: Fortalecer la seguridad de la información: proteger los datos y sistemas utilizados por las instituciones públicas contra amenazas internas y externas, mediante directrices actualizadas al respecto.

• Garantizar la continuidad operacional: asegurar que los servicios digitales del Estado operen de manera confiable y sin interrupciones críticas.

• Promover la interoperabilidad: hacer posible el intercambio seguro de información entre organismos estatales y los ciudadanos.

• Resguardar la privacidad: proteger los datos personales en concordancia con la normativa imperante en la materia.

De las discusiones sostenidas por los integrantes de la Dimensión se puede destacar:

Fortalezas:

• La normativa promueve la seguridad en procedimientos y expedientes electrónicos administrativos, siendo uno de los principios reconocidos en las plataformas electrónicas.

Desafíos:

• Variación en los niveles de madurez digital de los diversos organismos públicos que forman parte de la Administración del Estado.

• Preparación y capacitación del personal que deberá operar los sistemas informáticos implementados dentro de la administración del Estado.

• Elaborar medidas que permitan incorporar a aquellos miembros de la ciudadanía que tendrán dificultades para adaptarse a la transformación digital del Estado.

Propuestas:

• Crear criterios nacionales de madurez digital para estandarizar avances en los organismos públicos.

• Desarrollar programas de formación para poder tener niveles similares en los usuarios del sistema o plataformas electrónicas que permitan sustentar el procedimiento administrativo.

iii. Ley que establece el acceso a Internet como servicio público (Ley Nº 21.678).

La Ley N° 21.678, publicada el 3 de julio de 2024, establece el acceso a Internet como un servicio público de telecomunicaciones en Chile. Esta normativa modifica la Ley General de Telecomunicaciones (Ley N° 18.168) para incluir explícitamente el acceso a Internet dentro de los servicios públicos, asegurando su desarrollo armónico y equilibrado con la innovación tecnológica y la inversión privada.

Al reconocer el acceso a Internet como un servicio público esencial, la Ley N° 21.678 refuerza la necesidad de garantizar la seguridad y continuidad de este servicio. Esto implica que los proveedores de servicios de Internet deben implementar medidas de ciberseguridad adecuadas para proteger la infraestructura y los datos de los usuarios, asegurando una prestación segura y confiable del servicio. Además, la ley introduce sanciones más estrictas contra el daño o destrucción de la infraestructura de telecomunicaciones, lo que contribuye a la protección contra amenazas cibernéticas y físicas.

De la discusión sostenida, se pudo levantar:

Desafíos:

• Monopolios en zonas específicas del país.

• Limitaciones en infraestructura para expandir cobertura.

• Internet es una infraestructura necesaria para sustentar las interacciones en el ciberespacio, además de otras infraestructuras que participan en dicho proceso.

Propuestas:

• Incentivar la inversión privada y pública tanto en zonas rurales, como otras zonas de difícil acceso.

iv. Ley que promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros, Ley Fintec. (Ley Nº 21.521).

La Ley Nº 21.521 tiene por objeto establecer un marco para incentivar la prestación de servicios financieros a través de medios tecnológicos. Además, se reconoce un régimen jurídico para las plataformas de financiamiento colectivo; sistemas alternativos de transacción; asesoría crediticia y de inversión; custodia de instrumentos financieros; y enrutamiento de órdenes e intermediación de instrumentos financieros. La autoridad regulatoria a cargo de su implementación es la Comisión para el Mercado Financiero (CMF).

En particular, la normativa, en su Título III establece un estatuto jurídico para el Sistema de Finanzas Abiertas (SFA), que permite el intercambio de distintos prestadores de servicios de información de clientes financieros que haya consentimiento expresamente en ello y otros tipos de datos, mediante el uso de interfaces de acceso remoto y automatizado que permitan una interconexión y comunicación directa entre las instituciones participantes del SFA.

En particular, entre los elementos que deben cumplir las instituciones participantes se encuentran:

- Estándares de seguridad de información, especialmente mediante la adopción de medidas necesarias para cumplir con los estándares mínimos de seguridad de información, ciberseguridad, y políticas de gestión de riesgos y control interno, con el objeto de resguardar la confidencialidad, integridad y disponibilidad de los datos de la información y prevenir riesgos a los sistemas de información y prevenir riesgos a los sistemas de información que los procesan. Ante vulneraciones de las medidas de seguridad, las instituciones del SFA deberán reportar ante la Comisión para el Mercado Financiero.

- Consentimiento y sus requisitos, que establece requerimientos específicos para los proveedores de servicios basados en información y proveedores de servicios de iniciación de pago, mediante la adopción de mecanismos de autentificación del cliente y a través del consentimiento previo y explícito para la realización de consultas de información o iniciar pagos a su nombre, como el cese en su uso cuando haya sido revocado por el titular del dato. Además, las antes mencionadas instituciones serán responsables de resguardar la integridad, disponibilidad, seguridad y confidencialidad de los datos involucrados en cada transacción y adecuada privacidad de la información personal.

Durante el 2024, se publicó la Norma de Carácter General (NGC) Nº 514, que establece algunos lineamientos en relación a:

- Estándares de seguridad, respecto de la necesidad de contar con API que realicen procesos en condiciones de seguridad, lo que implica, contar con resguardos y respaldos adecuados de la información; mantener un registro actualizado de los eventos propios, en un período de 5 años; y eliminar correctamente la información una vez expiren los plazos legales.

- Consentimiento, que consiste en la voluntad expresa tanto de persona natural o jurídica. Las instituciones del SFA deben implementar mecanismos de autentificación y de gestión, almacenamiento de la voluntad en un soporte, y entregar información clara y precisa al cliente, especialmente respecto de los fines y en los procesos de transmisión, tratamiento o cesión de datos, así como la iniciación de pagos.

De la discusión sostenida, se pudo levantar:

Desafíos:

• Importancia de la coordinación regulatoria en el sector financiero en la implementación del Sistema de Finanzas Abiertos, en relación con las otras normativas discutidas a lo largo del presente Informe.

Propuestas:

• Promover el trabajo integrado entre las diversas autoridades para lograr estándares homogéneos y evitar la duplicidad de instrucciones, ya sean generales o específicas.

• Tomar las buenas prácticas y estándares internacionales en materia de seguridad de la información y gestión del consentimiento en el SFA.

4. CONCLUSIONES Y PASOS SIGUIENTES

→ Conclusiones

1. Marco integral y con desafíos de implementación: aunque Chile cuenta con un marco regulatorio robusto, enfrenta barreras significativas en términos de recursos y coordinación entre los diferentes actores. Adicionalmente, en los últimos años el país ha incorporado nuevas normativas que han conformado todo un ecosistema normativo que traen aparejados desafíos en la implementación, tanto para el sector público, como privado, sin considerar que este ecosistema se encuentra en expansión, como ocurre con las propuestas legislativas en materia de Inteligencia Artificial. Por ello, se requiere fortalecer y difundir, con carácter urgente, la cultura en ciberseguridad en el país. Además, se debiese fomentar el desarrollo de capacitación e implementación de sistemas de medición, homologación de criterios, para evaluar la madurez y cumplimiento y desempeño de las organizaciones en materia de legislación, regulación y estándares.

2. Necesidad de apoyo a PyMEs: es crucial proporcionar incentivos y herramientas para facilitar la transición de las PyMEs hacia el cumplimiento regulatorio, a través de programas de apoyo que incluyan financiamiento, asistencia técnica, capacitación y herramientas, para que puedan cumplir con las normativas de manera efectiva y protegerse adecuadamente contra las amenazas cibernéticas. En este mismo sentido, la homologación del trato diferenciado en materia de sanciones, que establece la Ley Marco de Ciberseguridad y la Ley de Protección de Datos Personales, respecto del apoyo de la(s) agencias, se debe centralizar también, en cuanto a las recomendaciones y plazo adicional para el cumplimiento de la legislación por parte de las PyMEs.

3. Apoyo a adultos mayores y NNA: es esencial que los esfuerzos públicos y privados permitan incorporar tanto a aquellos grupos que presentan bajos niveles de alfabetización digital como son los adultos mayores, así como fiscalizar la actividad que realizan los niños, niñas y adolescentes en los entornos digitales, quienes a pesar de tener mayores destrezas con la tecnología, no logran medir las consecuencias y la exposición de su información personal en el ciberespacio, la cual puede ser utilizada por agentes maliciosos para la comisión de diversos delitos. De esta manera, se debe propender a generar planes de concientización, capacitación que permitan un uso responsable y consciente por parte de estos actores.

4. Coordinación interinstitucional: la colaboración entre agencias como ANCI y la Agencia de Protección de Datos será esencial para garantizar la coherencia y eficacia en el cumplimiento de las Políticas de Ciberseguridad y de Protección de Datos Personales. Ambas agencias deben trabajar en estrecha colaboración para establecer políticas y normas complementarias, evitar redundancias y conflictos normativos y optimizar la supervisión y fiscalización. Además, esta colaboración es crucial para abordar de manera integral los desafíos actuales y futuros en materias de ciberseguridad y protección de datos, fomentando de paso, un entorno digital seguro y confiable para todos los ciudadanos. Adicionalmente, la canalización de reporte de incidentes de seguridad, y reporte de brechas de datos, a través del CSIRT Nacional, permite unificar criterios, facilitar la trazabilidad y seguimiento a la evolución de incidentes en todo el ecosistema.

5. Adopción de modelos de madurez: la implementación de este tipo de modelos en el tiempo es fundamental para el cumplimiento efectivo de la Ley Marco de Ciberseguridad, la Ley de Protección de Datos Personales y la Ley de Delitos Informáticos en Chile. Estos modelos permiten a las organizaciones evaluar su nivel de cumplimiento normativo, identificar brechas y establecer planes de mejora continuos. Al adoptar un enfoque gradual y basado en la medición, las organizaciones pueden fortalecer progresivamente sus capacidades de ciberseguridad, privacidad y gestión de riesgos, asegurando así una adaptación efectiva y sostenible a los requisitos legales en constante evolución.

Adicionalmente, es el Estado quien también debe adoptar indicadores que permitan medir el real cumplimiento de las normativas que componen el ecosistema digital en nuestro país.

→ Pasos Siguientes

1. Aprobar normativa reglamentaria pendiente: priorizar la implementación de reglamentos secundarios para la Ley Marco de Ciberseguridad que se encuentran actualmente en la Contraloría General de la República[4].

2. Capacitación y sensibilización: desarrollar programas nacionales para formar a profesionales en ciberseguridad y protección de datos de datos personales. Además, deben crearse iniciativas que involucren a la ciudadanía y a los escolares desde edad temprana en estas materias.

3. Monitoreo y evaluación: implementar sistemas estandarizados para medir la efectividad de las leyes en curso y con ello, contribuir a índices globales.

[4] Salvo aquellos que ya se encuentran aprobados mediante los Decretos Nº 275, 276 y 295 del 2024.

4. Integración en sistemas de compliance: facilitar la adopción de normativas a través de modelos de compliance organizacional, es decir, promover la autorregulación a través de modelos integrantes de cumplimiento de las normativas analizadas como aquellas que surjan a futuro.

En conclusión, si bien Chile cuenta con un marco legal robusto e integral en materia de ciberseguridad, persisten desafíos significativos en su implementación y coordinación. Resulta imperativo continuar fortaleciendo las capacidades nacionales en ciberseguridad, protección de datos personales y persecución de delitos informáticos. Es fundamental adoptar medidas concretas y articuladas que permitan superar estas brechas y consolidar un ecosistema digital seguro y resiliente para el desarrollo sostenible del país en el entorno tecnológico global.

Sin perjuicio de ello, importante es considerar la experiencia a nivel latinoamericano, especialmente tanto en Colombia como Brasil, donde la implementación de criterios y estándares puede conllevar una enorme resistencia por parte de algunas industrias, especialmente debido a la falta de coordinación regulatoria y al desconocimiento de los aspectos centrales de la normativa y los beneficios que conlleva para el resguardo de los derechos de la ciudadanía en el ciberespacio.

DIMENSIÓN 5:

Estándares y tecnologías 2024/2025

Moderadores:

Andrés Barrientos, Berioska Contreras Vargas, Gonzalo Díaz de Valdés, Jorge Astudillo Chávez, Josué Leiva Poblete, Leonardo Soto Cartes, Lorena Donoso, Luz Stella Cardona Meza, Matías Labbé, Patricio Leyton Roque, Peter Waher, Rudy Pinochet, Sebastián Rebolledo.

Autores y Moderadores:

- **Berioska Contreras Vargas - Universidad Técnica Federico Santa María.**
- **Peter Waher - Trust Anchor Group.**
- **Patricio Leyton Roque - Coordinador Eléctrico Nacional.**
- **Gonzalo Díaz de Valdés - Subsecretaría de Defensa.**
- **Rudy Pinochet - Presidente ISACA capítulo Santiago.**
- **Matías Labbé - Amazon Web Services.**
- **Luz Stella Cardona Meza - Universidad Nacional de Colombia - CIEP (Centro de**
- **investigación de ecosistemas de la Patagonia-Chile)**
- **Lorena Donoso - Aguas Antofagasta**
- **Andrés Barrientos - Cyber-Protection - Presidente - CECID Chile (Centro de estudios en**
- **ciberseguridad e investigación en defensa).**
- **Sebastián Rebolledo - Fundación 8dot8**
- **Jorge Astudillo Chávez - Sonda.**
- **Leonardo Soto Cartes - Capual.**
- **Josué Leiva Poblete (Editor) - Universidad Técnica Federico Santa María.**

→ 1. RESUMEN

El Foro Nacional de Ciberseguridad de Chile analiza el Dominio 5 (Estándares y Tecnologías) para fortalecer la ciberseguridad nacional. Este análisis revela desafíos cruciales, incluyendo la falta de un marco regulatorio robusto para la cadena de suministro, disparidades en la madurez de la ciberseguridad entre sectores y una gestión de riesgos débil, particularmente en las PYMEs. Se requiere un enfoque integral, que abarque el fortalecimiento del marco regulatorio, el fomento de una cultura de seguridad y el estímulo de la colaboración público-privada. El análisis también aborda los desafíos relacionados con el software, la resiliencia de Internet y el mercado de la ciberseguridad en Chile, proponiendo acciones específicas para cada área. Este informe proporciona un plan de acción conciso para implementar estrategias de ciberseguridad en Chile, incluyendo acciones convergentes con impacto nacional y un llamado a la acción para todos los sectores.

→ 2. ABSTRACT

Chile's National Cybersecurity Forum analyzes Domain 5 (Standards and Technologies) to strengthen national cybersecurity. This analysis reveals key challenges, including the lack of a robust regulatory framework for the supply chain, disparities in cybersecurity maturity across sectors, and weak risk management, particularly in SMEs. A comprehensive approach is required, encompassing strengthening the regulatory framework, fostering a security culture, and encouraging public-private collaboration. The analysis also addresses challenges related to software, Internet resilience, and the cybersecurity market in Chile, proposing specific actions for each area. This report provides a concise action plan for implementing cybersecurity strategies in Chile, including converging actions with national impact and a call to action for all sectors.

→ 3. INTRODUCCIÓN

El Foro Nacional de Ciberseguridad en Chile (ForoCiber) se crea con el propósito de establecer un entorno de colaboración público-privado permanente. Más aún, esta plataforma busca ser un espacio de diálogo y colaboración para fortalecer la ciberseguridad en este país, abordando los desafíos desde múltiples perspectivas y promoviendo el desarrollo de capacidades y políticas en esta materia. El Modelo de Madurez de las Capacidades de Ciberseguridad (CMM) de la Universidad de Oxford ayuda al ForoCiber a proporcionar un marco estructurado y completo para evaluar y mejorar las capacidades de ciberseguridad del país.

El presente escrito aborda el Dominio 5 de Estándares y Tecnologías. Este dominio se centra en fortalecer la ciberseguridad del país a través de la promoción y desarrollo de estándares, tecnologías y buenas prácticas en el ámbito de la seguridad de la información. Su principal objetivo es discutir, compartir conocimiento y proponer iniciativas que mejoren la protección de la infraestructura crítica nacional y presentar recomendaciones o cursos de acción que permitan apoyar las decisiones en materia de política pública.

El capítulo de Metodología Aplicada describe el proceso de trabajo del equipo, incluyendo los objetivos, la organización y los métodos de análisis de información. Para lograr estos objetivos se propone un plan estratégico con acciones concretas para abordar los desafíos identificados en cada área, con el objetivo de fortalecer la ciberseguridad en Chile.

Cada uno de los seis factores clave se analiza en un capítulo independiente. Cada capítulo de los factores del Dominio 5 presenta un panorama general o contexto, los principales desafíos y oportunidades, y las medidas concretas para abordar dichos hallazgos.

El capítulo de Cumplimiento de estándares aborda la necesidad de un marco regulatorio, la madurez de la ciberseguridad en diferentes sectores, la gestión de riesgos y las barreras para la adopción de estándares. El capítulo de Controles de seguridad analiza los incidentes de seguridad comunes y propone controles esenciales para la protección de la información. El capítulo de Calidad del software evalúa las metodologías y herramientas para asegurar la calidad del software, la gestión de requisitos y los procesos de actualización y mantenimiento. El capítulo de Resiliencia de la infraestructura de Internet examina la confiabilidad y protección de la infraestructura, incluyendo la evaluación y monitoreo de la resiliencia de la red. El capítulo de Mercado de ciberseguridad analiza el crecimiento, madurez y principales actores del mercado en Chile, y el capítulo de Divulgación responsable explora la importancia de un marco de divulgación responsable para la información sobre vulnerabilidades. Por último, se presentan las conclusiones más significativas y las referencias de distintas fuentes de información.

→ 4. METODOLOGÍA APLICADA

→ 4.1. OBJETIVO GENERAL Y ESPECÍFICOS

El Dominio 5 de estándares y tecnologías es un pilar estratégico del Foro Ciber, que mediante una gobernanza colaborativa, el análisis detallado de sus seis factores, y el desarrollo de recomendaciones normativas y técnicas, busca proteger la infraestructura crítica y fomentar un ecosistema digital robusto y seguro para todos.

Para proteger los servicios vitales y promover un entorno digital seguro y confiable se necesita responder a las siguientes áreas específicas:

- Establecer una gobernanza y una estrategia colaborativa del grupo de expertos.
- Analizar la situación de los seis factores del dominio para identificar hallazgos relevantes.
- Recomendar iniciativas y medios de cumplimiento efectivo del marco normativo.

→ 4.2. ORGANIZACIÓN DEL DOMINIO 5

Las capacidades del dominio quinto de estándares y tecnologías consiste en personas que han desarrollado expertís en los distintos subdominios que incluyen la adherencia a estándares, controles de seguridad, calidad del software, resiliencia en la infraestructura de comunicaciones e Internet, el mercado de la ciberseguridad y la divulgación responsable de datos. Es decir, este es el único dominio que abarca seis subcategorías, siendo el más extenso, multidimensional y complejo de todos. La siguiente tabla presenta la asignación actualizada de moderadores por factor:

Factor de Dominio 5	Miembros Moderadores
D 5.1: Cumplimiento de los estándares	Patricio Leyton Roque
	Gonzalo Díaz de Valdés O.
D 5.2: Controles de seguridad	Rudy Pinochet
	Matías Labbé
D 5.3: Calidad del software	Luz Stella Cardona
	Lorena Donoso Ubilla
D 5.4: Comunicaciones e Internet Resiliencia	Berioska Contreras Vargas
de la infraestructura	Peter Waher
D 5.5: Mercado de ciberseguridad	Andrés Barrientos
	Sebastián Rebolledo
D 5.6: Divulgación responsable	Jorge Astudillo Chávez
	Leonardo Soto Cartes

Figura: Moderadores Activos del Dominio 5

La organización y coordinación de los esfuerzos sigue una dinámica democrática donde cada moderador tiene voz y voto. Cada idea se considera cuidadosamente, se discuten abiertamente las ventajas y desventajas, y se exploran diferentes perspectivas. El objetivo no es simplemente llegar a un acuerdo rápido, sino asegurarse de que todos se sientan escuchados y comprendidos. La participación activa de cada moderador es esencial para progresar con los objetivos del equipo, y por esta razón, definimos un Protocolo de Participación de Moderadores Activos, el cual define que ante la inactividad consecutiva de un moderador, debido a una eventual sobrecarga laboral, su rol será cedido a otro participante activo, propuesto y aceptado por el equipo, es decir, se desinscribe el rol moderador y cambia a participante.

En julio de 2024, el desempeño del equipo lograba movilizar los esfuerzos de cerca del 30% de sus moderadores, y en septiembre de 2024 logramos movilizar al 100% de sus moderadores con el nuevo Protocolo, lo que nos permite distribuir de manera equitativa los esfuerzos y tomar acciones oportunas ante algún subdominio rezagado. Es decir, ha existido un necesario cambio en la asignación original de moderadores, siendo la asignación de octubre de 2024 distinta de aquella presentada en julio del mismo año.

Un aspecto relevante en la orgánica del equipo son las reuniones bisemanales, esta frecuencia ha resultado ser flexible para los moderadores, y en el período de junio a octubre se completaron diez sesiones fomentando la productividad del equipo.

En relación con las iniciativas de difusión del dominio, el equipo incluyó medios como las redes sociales para expandir su impacto, como lo es Discord para abrir un espacio de interacción más diverso y realizar las sesiones bisemanales. Así como, LinkedIn para propagar encuestas temáticas.

→ 4.3. IDENTIFICACIÓN Y ANÁLISIS DE HALLAZGOS

El Protocolo de Participación también recopila y analiza indicadores relevantes que permiten tomar una decisión informada al equipo, un ejemplo de esto es el seguimiento del número de participantes por cada Dominio. Este indicador demuestra que en el periodo entre Julio de 2024 y Marzo de 2025, el número de participantes aumentó un 40%, desde 180 participantes en un inicio, hasta 253 participantes, siendo el dominio de mayor participación del ForoCiber.

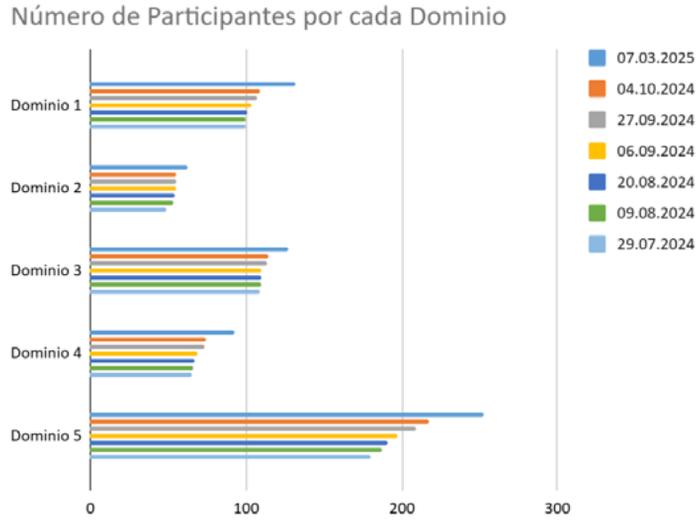


Figura: Número de Participantes por Dominio

Otro indicador significativo es el número de hilos por cada factor de este dominio, en donde se han aplicado dos métodos de selección de tema de discusión; la exposición de un caso real y la validación previa del tema a través de encuestas.

Presentar un hilo de discusión basado en un caso ofrece varias ventajas, primero expone un incidente y una respuesta real capturando mayor atención que un ejemplo hipotético. Al analizar un caso real, se pueden explorar las complejidades y los matices de un tema de manera más tangible, a su vez, podemos proporcionar antecedentes concretos y respaldarlos con argumentos convincentes que aumentan la credibilidad del hilo de discusión.

Por otro lado, validar un tema de un hilo de discusión previamente en redes sociales como LinkedIn nos permite asegurar la relevancia con un público objetivo. Una encuesta arroja tendencias que nos ayudan a observar las reacciones y comentarios para determinar si el tema genera interés y debate. Las encuestas de validación temática ayudan a evitar invertir tiempo en un hilo que podría no tener el impacto deseado. Más aún, a través de la interacción en LinkedIn se pueden identificar personas con experiencia o interés en el tema que podrían colaborar en el hilo, enriqueciendo la discusión con diferentes perspectivas. Una vez generado suficiente interés, el contenido puede ser compartido aumentando la visibilidad del hilo de discusión.

En la siguiente ilustración es posible notar que **todos los factores han presentado, al menos, un hilo** de discusión en el periodo evaluado, y que alcanza un **máximo de 11 hilos** de discusión para el factor D5.6 Divulgación Responsable, seguido del factor D5.4: Comunicaciones e Internet Resiliencia de la infraestructura con **6 hilos.**

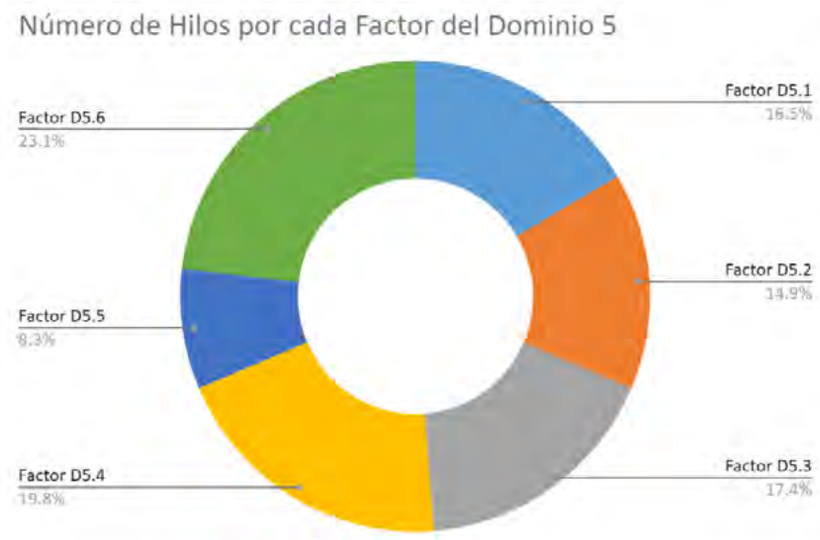


Figura: Número de Hilos por Factor

Por último, el número de respuestas recibidas por cada hilo del dominio nos permite tomar la decisión de aumentar o no el número de hilos y analizar sus resultados. Sin embargo, es posible notar que un mayor número de hilos no garantiza un mayor número de respuestas como demuestra el indicador ilustrado. En general, el rango de respuestas recibidas por el dominio 5 oscila entre **5 y 28 respuestas** por hilo, con una media de **14** respuestas.

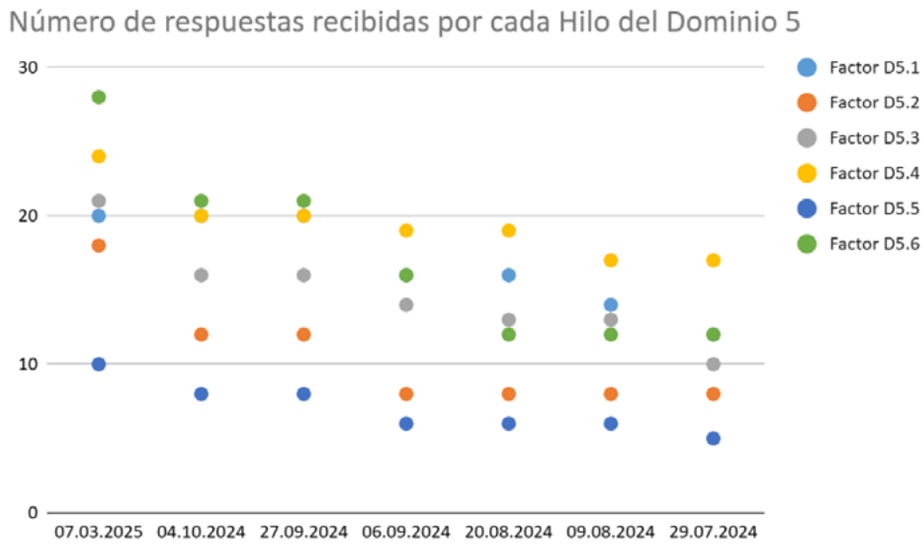


Figura: Número de Respuestas por Factor

→ 4.4. PLAN ESTRATÉGICO DEL DOMINIO 5

Esta Dimensión consiste en medidas efectivas y generalizadas del uso de tecnología de ciberseguridad para proteger a las personas, organizaciones e infraestructura nacional. La dimensión examina específicamente la implementación de la ciberseguridad, estándares y buenas prácticas, el despliegue de procesos y controles, y el desarrollo de tecnologías y productos para reducir los riesgos de la seguridad digital.

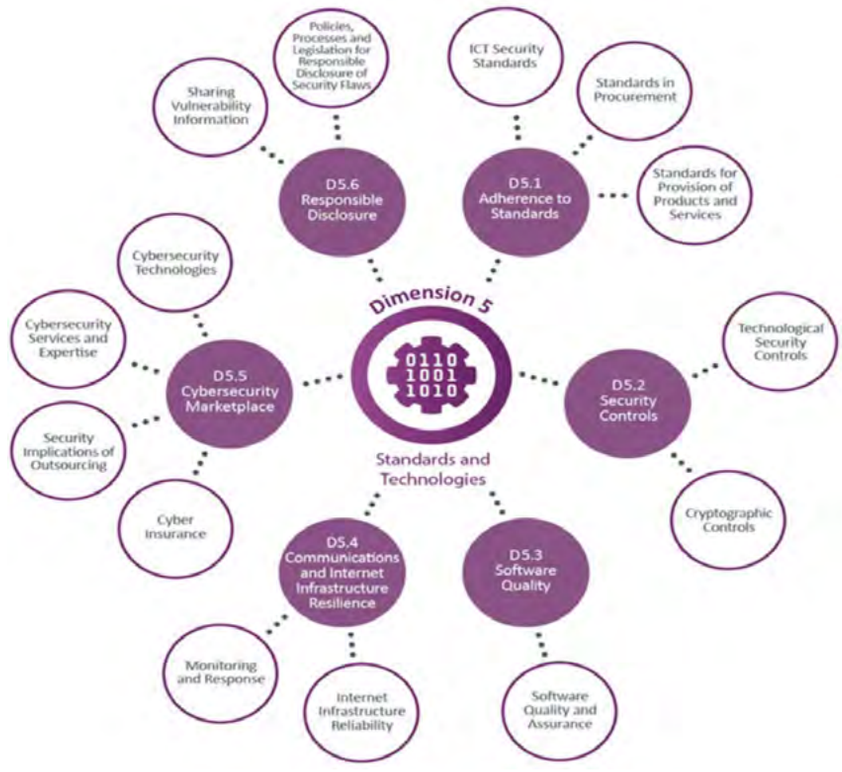


Figura: Alcance del Roadmap

El plan representa un proceso progresivo de seis etapas que transcurren entre julio 2024 y diciembre 2025. Tal proceso inicia con la consolidación del equipo estableciendo e implementando el Protocolo de Participación de Moderadores Activos. Luego, es propuesta la primera versión del diseño de planificación para el período 2024-2025 que recibe como principal entrada los hallazgos identificados en los hilos de discusión, siendo un documento modular basado en seis factores que son actualizados gradualmente. La tercera etapa documenta el análisis de hallazgos y las acciones recomendadas que son consolidadas en un reporte público. La cuarta etapa es la presentación y difusión de los resultados. La quinta y sexta etapa son iteraciones que permitirán contrastar avances y examinar el impacto de las acciones para desarrollar un nuevo plan detallado.

Figura: Línea de Tiempo del Roadmap

4.4.1. FACTOR D.5.1 - ADHERENCIA A LOS ESTÁNDARES

Este factor evalúa la capacidad del gobierno para promover, evaluar la implementación y monitorear el cumplimiento de los estándares y buenas prácticas internacionales de ciberseguridad. Este factor se divide en tres aspectos:

- **Estándares de seguridad de las TIC:** examina si los estándares y las buenas prácticas relacionados con la ciberseguridad se están implementando de manera generalizada en el sector público y las organizaciones de infraestructura crítica.

- **Estándares en adquisiciones:** aborda la implementación de estándares y buenas prácticas en todos los sectores para guiar los procesos de adquisición, incluida la gestión de riesgos, la gestión del ciclo de vida, la garantía de software y hardware, la externalización y el uso de servicios en la nube.

- **Estándares para el suministro de productos y servicios:** aborda el uso de estándares y buenas prácticas por parte de los proveedores locales de bienes y servicios, incluidos software, hardware, servicios gestionados y servicios en la nube.

4.4.2. FACTOR D.5.2 - CONTROLES DE CIBERSEGURIDAD

Este factor examina la implementación de controles de seguridad por parte de los usuarios y los sectores público y privado, y si el conjunto de controles de ciberseguridad tecnológicos se basa en marcos de ciberseguridad establecidos. Este factor se divide en dos aspectos:

• **Controles de seguridad tecnológicos:** explora en qué medida se implementan controles de seguridad tecnológicos actualizados, incluyendo parches y copias de seguridad, en todos los sectores.

• **Controles criptográficos:** revisa la implementación de técnicas criptográficas en todos los sectores y usuarios para la protección de datos en reposo o en tránsito, y en qué medida estos controles criptográficos cumplen con los estándares y directrices internacionales y se mantienen actualizados.

4.4.3. FACTOR D.5.3 - CALIDAD DEL SOFTWARE

Este factor examina la calidad de la implementación del software y los requisitos funcionales en los sectores público y privado. Además, revisa la existencia y mejora de las políticas y procesos de actualizaciones y mantenimiento de software basados en evaluaciones de riesgos y la naturaleza crítica de los servicios. Este factor se compone de un único aspecto:

• **Calidad y garantía del software:** aborda la calidad y los requisitos funcionales del software utilizado en el país, así como las políticas y procesos relacionados con las actualizaciones y el mantenimiento del software, incluida la gestión de parches.

4.4.4. FACTOR D.5.4 - RESILIENCIA DE LAS COMUNICACIONES Y LA INFRAESTRUCTURA E INTERNET

Este factor aborda la existencia de servicios e infraestructura de Internet confiables en el país, así como procesos de seguridad rigurosos en los sectores público y privado. Además, revisa el control que el gobierno podría tener sobre su infraestructura de Internet y en qué medida las redes y los sistemas están subcontratados. Este factor se divide en dos aspectos:

• **Confiabilidad de la infraestructura de Internet:** examina la confiabilidad y protección de los servicios e infraestructura de Internet en los sectores público y privado.

• **Monitoreo y respuesta:** examina si existen mecanismos para realizar evaluaciones de riesgos y monitorear la resiliencia de la red tanto en los sectores público como privado.

4.4.5. FACTOR D.5.5 - MERCADO DE CIBERSEGURIDAD

Este factor aborda la disponibilidad y el desarrollo de tecnologías de ciberseguridad competitivas, productos de ciberseguros, servicios de ciberseguridad y experiencia, y las implicaciones de seguridad de la externalización. Este factor se divide en cuatro aspectos:

• **Tecnologías de ciberseguridad:** examina si existe y se apoya un mercado nacional de tecnologías de ciberseguridad, informado por las necesidades nacionales.

• **Servicios y experiencia en ciberseguridad:** explora la disponibilidad de servicios de consultoría en ciberseguridad para organizaciones privadas y públicas.

• **Implicaciones de seguridad de la externalización:** examina si se realizan evaluaciones de riesgos para determinar cómo mitigar los riesgos de externalizar las TI a un tercero o a servicios en la nube.

• **Ciberseguros:** explora la existencia de un mercado de ciberseguros, su cobertura y productos adecuados para diversas organizaciones.

4.4.6. FACTOR D.5.6 - DIVULGACIÓN RESPONSABLE

Este factor explora el establecimiento de un marco de divulgación responsable para la recepción y difusión de información sobre vulnerabilidades en todos los sectores, y si existe la capacidad suficiente para revisar y actualizar continuamente este marco. Este factor se divide en dos aspectos:

• **Intercambio de información sobre vulnerabilidades:** explora los mecanismos o canales existentes para el intercambio de información sobre los detalles técnicos de las vulnerabilidades entre las partes interesadas.

• **Políticas, procesos y legislación para la divulgación responsable de fallas de seguridad:** explora la existencia de una política o marco de divulgación responsable en las organizaciones de los sectores público y privado, y el derecho a la protección legal de quienes divulgan fallas de seguridad.

→ 4.5 RETROALIMENTACIÓN INFORME SEGUNDO AVANCE

Con fecha 18 de diciembre de 2024, el presente informe en su primera versión recibió la aceptación de publicación sin observaciones, con espacio para mejoras voluntarias. El equipo optó consensuadamente por revisar el informe en tres sesiones para dar forma a esta versión final pensada para ser presentada en el Tercer Avance del Foro Nacional de Ciberseguridad, el día 14 de abril de 2025:

• Primera sesión de revisión: 10 de enero de 2025, objetivo identificar mejoras para cada factor de manera individual.

• Segunda sesión de revisión: 24 de enero de 2025, objetivo identificar mejoras para integrar factores, surgiendo el capítulo de Convergencia de Acciones con Impacto Nacional.

• Tercera Sesión de revisión: 07 de marzo de 2025, objetivo consensuar cambios y editar.

→ 5. FACTOR D.5.1: CUMPLIMIENTO DE LOS ESTÁNDARES

→ 5.1. CONTEXTO

En un mundo cada vez más interconectado y dependiente de la tecnología, las amenazas de ciberseguridad representan uno de los riesgos más graves para la continuidad y confiabilidad de las cadenas de suministro en Chile y en todo el mundo. Con la convergencia de los sistemas de tecnología de la información (TI) y tecnología operativa (TO), que incluye desde sistemas administrativos hasta equipos y procesos industriales, las industrias enfrentan desafíos complejos en la protección de sus activos. La cadena de suministro es particularmente vulnerable, ya que está formada por múltiples actores y nodos interdependientes que, al estar interconectados, pueden convertirse en posibles puntos de entrada para ataques cibernéticos.

En Chile, la ciberseguridad ha ganado relevancia en sectores críticos como energía, telecomunicaciones, banca y salud, pero aún no existen normativas estándar y desplegadas que se enfoquen específicamente en la ciberseguridad de la cadena de suministro en todas las industrias.

Actualmente, la mayoría de las empresas se basan en estándares internacionales como el NIST (National Institute of Standards and Technology), la norma ISO/IEC 27001, NERC-CIP o el estándar IEC 62443 para sistemas industriales. Sin embargo, la implementación de un modelo de cumplimiento y la definición de estándares específicos para el contexto chileno es un desafío complejo que requiere la colaboración entre el sector público, el privado y los organismos reguladores.

→ 5.2. HALLAZGOS

5.2.1 FALTA DE UN MARCO REGULATORIO NACIONAL PARA CIBERSEGURIDAD EN TI Y TO EN LA CADENA DE SUMINISTRO.

A pesar de que Chile ha avanzado en la creación de regulaciones y estándares de ciberseguridad en sectores específicos, como la banca (a través de la CMF - Comisión para el Mercado Financiero) o el sector energético (con la CNE - Comisión Nacional de Energía), aún no se cuenta con un enfoque normativo específico para la cadena de suministro y la convergencia TI/TO. La ausencia de una legislación integral dificulta la estandarización de prácticas y el desarrollo de una estrategia uniforme en todas las industrias. Esto se traduce en una dependencia de estándares internacionales que, aunque útiles, no están adaptados completamente al contexto local ni a la infraestructura y capacidades técnicas del país.

5.2.2 DIVERSIDAD DE MADUREZ EN CIBERSEGURIDAD ENTRE SECTORES INDUSTRIALES Y SU CADENA DE SUMINISTRO.

La madurez de ciberseguridad varía significativamente entre los sectores industriales en Chile. Mientras que el sector energético, bancario y el de telecomunicaciones han realizado importantes inversiones en infraestructura y cumplimiento de normas, sectores como el comercio minorista, servicios de salud primaria, entre otros; presentan menores niveles de protección y desconocimiento sobre los estándares.

Este contexto crea un entorno heterogéneo en el cual los sectores avanzados adoptan medidas de protección que no se replican en toda la cadena de suministro, generando así puntos vulnerables en los eslabones más débiles de la cadena.

5.2.3 DÉBIL GESTIÓN DE RIESGOS EN LA CADENA DE SUMINISTRO.

La ciberseguridad en la cadena de suministro no solo depende de las prácticas de seguridad de la empresa principal, sino de la capacidad de todos sus proveedores para implementar medidas de protección efectivas.

En Chile, las pequeñas y medianas empresas (PYMES), que constituyen la mayor parte de la cadena de suministro, suelen tener menos recursos y conocimiento para implementar estándares de ciberseguridad robustos. La falta de evaluaciones regulares de riesgo y de una cultura de seguridad compartida entre las empresas de la cadena, limita la posibilidad de implementar una estrategia unificada que mitigue los riesgos asociados a la conectividad e infraestructura TI/TO.

5.2.4 BARRERAS TÉCNICAS Y ECONÓMICAS EN LA CADENA DE SUMINISTRO.

Implementar una infraestructura de ciberseguridad sólida en TI y TO exige una inversión significativa en hardware, software y capacitación. En muchos casos, las empresas en Chile enfrentan restricciones económicas para actualizar sus sistemas o contratar personal especializado. Esto es especialmente relevante en TO, donde la tecnología suele estar compuesta por equipos antiguos, cuya actualización o reemplazo es costosa. Además, la falta de especialistas en ciberseguridad en TO limita la capacidad de implementación de medidas efectivas.

5.2.5 DEPENDENCIA DE LA CADENA DE SUMINISTRO INTERNACIONAL.

Chile es un país altamente dependiente de las importaciones y exportaciones, y muchos de los productos o componentes en su cadena de suministro provienen de otros países. La interconexión con socios comerciales internacionales añade complejidad, ya que muchas empresas en la cadena no están sujetas a los mismos estándares de ciberseguridad o tienen niveles de cumplimiento diversos. Esto aumenta la exposición a vulnerabilidades que pueden propagarse rápidamente a través de la cadena de suministro global.

5.2.6 SERVICIOS DIGITALES DE PROVEEDORES FUERA O DENTRO DEL TERRITORIO NACIONAL.

Se han evidenciado en los los últimos años, incidentes de ciberataque de alto impacto en servicios esenciales u operadores de importancia vital (como salud, compras públicas, entre otros) en el cual ha estado involucrada la cadena de suministro de servicios digitales como Datacenters, lo cual hace indispensable considerar estándares mínimos para una operación segura que de ciertas garantías a las entidades mandantes y críticas en un escenario de amenaza, que pudiese poner en riesgo uno o más servicios esenciales.

→ 5.3. ACCIONES

Para abordar los desafíos identificados y avanzar hacia un modelo de ciberseguridad efectivo en TI y TO en la cadena de suministro, se proponen las siguientes acciones:

5.3.1 GOBERNANZA DE CIBERSEGURIDAD EN ESTÁNDARES Y CUMPLIMIENTO EN LA CADENA DE SUMINISTROS.

Con la nueva institucionalidad contenida en la Ley N° 21.663 Marco de Ciberseguridad resulta ser necesario que la articulación y visión sistémica para la definición, implementación, monitoreo y verificación de cumplimiento de estándares para múltiples proveedores de la cadena de suministro en diversos sectores industriales, se desarrolle de forma integral, sistémica y que sea escalable en conjunto con el avance que deben cumplir las entidades mandantes, bajo los requisitos regulatorios que impondrá la Ley Marco de Ciberseguridad.

5.3.2 PROFUNDIZAR EL MARCO REGULATORIO NACIONAL DE CIBERSEGURIDAD.

La creación de un marco regulatorio específico para ciberseguridad en ambientes TI/TO en la cadena de suministro es esencial. Este marco debe estar alineado con estándares internacionales, pero adaptado a las necesidades y capacidades de las empresas chilenas. Iniciativas como la Ley N° 21.663 Marco de Ciberseguridad, representan una oportunidad para establecer lineamientos específicos para la protección de sistemas críticos en la cadena de suministro, tanto en servicios esenciales como en operadores de importancia vital.

5.3.3 FOMENTAR LA CULTURA DE SEGURIDAD Y LA GESTIÓN DE RIESGOS.

Es importante fortalecer la cultura de ciberseguridad en toda la cadena de suministro, no solo en las grandes empresas, sino también en las PYMES y proveedores menores. Esto puede lograrse a través de campañas de concientización, capacitaciones y el fomento de prácticas de gestión de riesgos que incluyan la realización de auditorías y evaluaciones de seguridad de manera regular.

5.3.4 CREAR INCENTIVOS ECONÓMICOS Y FINANCIEROS.

La implementación de medidas de ciberseguridad requiere recursos, y no todas las empresas tienen la capacidad de hacer frente a los costos. El Estado chileno puede ofrecer incentivos financieros, tales como créditos fiscales, subvenciones o préstamos con tasas de interés preferenciales, así como la participación en fondos concursables que propicien el desarrollo de la ciberseguridad en todos los sectores industriales, facilitando que las empresas inviertan en tecnologías de ciberseguridad en TI y TO. Esto también incluye la capacitación de profesionales en ciberseguridad, ya que el país enfrenta una escasez de especialistas en este campo.

5.3.5 IMPLEMENTAR PROGRAMAS DE COLABORACIÓN PÚBLICO-PRIVADA.

La colaboración entre el sector público y privado es clave para fortalecer la ciberseguridad en la cadena de suministro. Programas de colaboración en los cuales las empresas compartan información sobre amenazas y vulnerabilidades, y reciban asistencia técnica para implementar medidas de protección, pueden ser de gran ayuda para fortalecer la resiliencia de las industrias. Iniciativas como el CSIRT (Centro de Respuesta ante Incidentes de Seguridad Informática) se pueden expandir, priorizando la

creación de CSIRTs sectoriales, un paso correcto en la dirección adecuad, para el logro del objetivo de fortalecimiento y adaptación a las necesidades específicas de ciberseguridad TI y TO en la cadena de suministros.

5.3.6 ADOPTAR TECNOLOGÍAS DE SEGURIDAD AVANZADA.

Incorporar tecnologías como la segmentación de redes, la inteligencia artificial (IA) y el aprendizaje automático (ML) pueden ayudar a detectar y mitigar amenazas de manera proactiva. La implementación de una arquitectura de seguridad de confianza cero (Zero Trust Architecture), que se basa en la verificación continua de usuarios y dispositivos en la red, es fundamental para reducir las posibilidades de intrusión en sistemas críticos. Además, los sistemas de monitoreo continuo y la integración de soluciones de seguridad en TI y TO ayudarán a detectar ataques en tiempo real.

La ciberseguridad en ambientes de TI y TO en la cadena de suministro es un desafío que requiere una estrategia integral y adaptada al contexto chileno. Si bien, existen estándares internacionales que se han adoptado y adaptado a la realidad nacional como NERC-CIP en el sector eléctrico, estos estándares pueden y deben guiar a las empresas en su práctica, siendo aún necesario un marco regulatorio nacional que promueva un nivel de cumplimiento uniforme. La implementación de este modelo exige colaboración entre el sector público y privado, incentivos económicos y un esfuerzo continuo de capacitación en ciberseguridad.

Finalmente concluimos que, sólo a través de un enfoque integral que considere la especificidad de cada sector, la diversidad en la madurez de ciberseguridad y la naturaleza interdependiente de las cadenas de suministro, Chile podrá avanzar hacia una protección eficaz y una mayor resiliencia nacional frente a las amenazas cibernéticas en todos los sectores industriales.

Además resulta fundamental que dentro del rol que cumplirá la Agencia Nacional de Ciberseguridad (ANCI), se le otorgue prioridad a la gobernanza y a la cadena de suministro, con el propósito de abordarlo desde una etapa temprana a la puesta en marcha de la Ley Marco de Ciberseguridad.

→ 6. FACTOR D.5.2: CONTROLES DE SEGURIDAD

→ 6.1. CONTEXTO

En la actualidad se han presentado incidentes y riesgos en nuestro país y en el mundo, los cuales han proliferado y evolucionado cada vez más rápido con la llegada de la inteligencia artificial y el desarrollo e implementación de nuevas arquitecturas tecnológicas en las distintas verticales de negocio, defensa y gobierno. Esto nos impulsa a evaluar y definir una serie de controles de seguridad generales y esenciales en orden de prioridad para que sean plasmados en todo tipo de organización como línea base.

→ 6.2. HALLAZGOS

Según el panorama de incidentes de seguridad que se ha presentado en los últimos años en nuestro país, y cómo este se contrasta con la evolución de las tecnologías y su implementación en la industria de soluciones, se identificaron diez puntos esenciales que fueron la causa de aquellos fallos de seguridad e impacto en la operación, los cuales se detallan a continuación:

6.2.1 Exfiltración de datos y credenciales de plataformas tecnológicas provistas por entidades públicas y privadas.

6.2.2 Pérdidas y acceso indebido de información privada de ciudadanos por medio de ataques a los servicios y sistemas de instituciones tanto privadas como públicas.

6.2.3 Migración e integración de servicios on-premise en proveedores de nube manteniendo la misma arquitectura de seguridad sin una correcta evaluación del nuevo panorama de amenazas.

6.2.4 Falta de protocolos organizacionales y equipos integrales preparados para atender incidentes de seguridad a nivel transversal para identificar, proteger, detectar, responder y recuperar servicios.

6.2.5 Educación y evaluación constante de los distintos vectores de ataque a todos los usuarios tanto internos como externos a la organización, según su rol, riesgos inherentes de su actividad y participación en la operación de las instituciones.

6.2.6 Evaluación constante tanto interna como externa de brechas de seguridad, aseguramiento durante todo el proceso de creación, modificación, puesta en marcha y continuidad de soluciones tecnológicas tanto nuevas como existentes, en base a los riesgos, privacidad y criticidad de estas.

6.2.7 Generación de una defensa a nivel de capas (defensa en profundidad) y a nivel organizacional según los riesgos, privacidad, prioridad y panoramas de amenazas que estos servicios durante todo el proceso de recolección, procesamiento, transporte, entrega y acceso según su sensibilidad.

6.2.8 Actualización de plataformas y sistemas a nivel de capas, aplicación de buenas prácticas de mercado según criticidad, privacidad, sensibilidad, resguardo y riesgos inherentes a su función dentro de las organizaciones.

6.2.9 La falta de controles por medio de entes reguladores de pruebas, evaluación, evidencias de restauración de servicios, datos asociados a la organización y sus clientes/usuarios según las características del negocio.

6.2.10 La falta de preparación y evaluación de los equipos de seguridad y resguardo, controles tecnológicos de las organizaciones a nivel de acceso físico a sus dependencias de personal externo e interno por medio de pruebas de penetración por parte de terceros especializados.

creación de CSIRTs sectoriales, un paso correcto en la dirección adecuad, para el logro del objetivo de fortalecimiento y adaptación a las necesidades específicas de ciberseguridad TI y TO en la cadena de suministros.

5.3.6 ADOPTAR TECNOLOGÍAS DE SEGURIDAD AVANZADA.

Incorporar tecnologías como la segmentación de redes, la inteligencia artificial (IA) y el aprendizaje automático (ML) pueden ayudar a detectar y mitigar amenazas de manera proactiva. La implementación de una arquitectura de seguridad de confianza cero (Zero Trust Architecture), que se basa en la verificación continua de usuarios y dispositivos en la red, es fundamental para reducir las posibilidades de intrusión en sistemas críticos. Además, los sistemas de monitoreo continuo y la integración de soluciones de seguridad en TI y TO ayudarán a detectar ataques en tiempo real.

La ciberseguridad en ambientes de TI y TO en la cadena de suministro es un desafío que requiere una estrategia integral y adaptada al contexto chileno. Si bien, existen estándares internacionales que se han adoptado y adaptado a la realidad nacional como NERC-CIP en el sector eléctrico, estos estándares pueden y deben guiar a las empresas en su práctica, siendo aún necesario un marco regulatorio nacional que promueva un nivel de cumplimiento uniforme. La implementación de este modelo exige colaboración entre el sector público y privado, incentivos económicos y un esfuerzo continuo de capacitación en ciberseguridad.

Finalmente concluimos que, sólo a través de un enfoque integral que considere la especificidad de cada sector, la diversidad en la madurez de ciberseguridad y la naturaleza interdependiente de las cadenas de suministro, Chile podrá avanzar hacia una protección eficaz y una mayor resiliencia nacional frente a las amenazas cibernéticas en todos los sectores industriales.

Además resulta fundamental que dentro del rol que cumplirá la Agencia Nacional de Ciberseguridad (ANCI), se le otorgue prioridad a la gobernanza y a la cadena de suministro, con el propósito de abordarlo desde una etapa temprana a la puesta en marcha de la Ley Marco de Ciberseguridad.

→ 6. FACTOR D.5.2: CONTROLES DE SEGURIDAD

→ 6.1. CONTEXTO

En la actualidad se han presentado incidentes y riesgos en nuestro país y en el mundo, los cuales han proliferado y evolucionado cada vez más rápido con la llegada de la inteligencia artificial y el desarrollo e implementación de nuevas arquitecturas tecnológicas en las distintas verticales de negocio, defensa y gobierno. Esto nos impulsa a evaluar y definir una serie de controles de seguridad generales y esenciales en orden de prioridad para que sean plasmados en todo tipo de organización como línea base.

→ 6.3. ACCIONES

De acuerdo con los hechos antes descritos, se proponen los siguientes diez ámbitos y elementos de apoyo a ser implementados y considerados como línea base en toda organización e industria:

6.3.1 Gestión de Identidades y Accesos (IAM):

• **Autenticación multifactor:** Implementación obligatoria para todos los accesos críticos.

• **Principio de mínimo privilegio:** Otorgar únicamente los permisos necesarios a cada usuario.

• **Gestión de sesiones:** Establecer tiempos máximos de inactividad y monitorear las actividades de los usuarios.

• **Gestión de contraseñas sólidas:** Políticas estrictas para la creación y rotación de contraseñas.

6.3.2 Cifrado:

• **Cifrado de datos en reposo:** Proteger la información almacenada en discos duros, bases de datos y otros medios.

• **Cifrado de datos en tránsito:** Asegurar la confidencialidad de los datos durante su transmisión por redes.

• **Cifrado de dispositivos móviles:** Proteger la información almacenada en dispositivos personales.

6.3.3 Seguridad de la Nube:

• **Modelado de amenazas:** Identificar y evaluar los riesgos específicos de cada entorno en la nube.

• **Segmentación de redes:** Aislar los recursos en la nube para limitar el impacto de posibles brechas.

• **Gestión de vulnerabilidades:** Mantener actualizados los sistemas y aplicar parches de seguridad.

6.3.4 Detección y Respuesta a Incidentes:

• **Sistemas de detección de intrusiones (IDS):** Monitorear la red en busca de actividades sospechosas.

• **Análisis de registros:** Revisar los registros de eventos para identificar patrones de ataque.

• **Planes de respuesta a incidentes:** Establecer procedimientos claros y concisos para responder a incidentes de seguridad

6.3.5 Concientización y Capacitación de los Usuarios:

• **Programas de capacitación continuos:** Educar a los empleados sobre las últimas amenazas y cómo prevenirlas.

• **Simulaciones de ataques:** Evaluar la efectividad de los programas de capacitación y la capacidad de respuesta de los empleados.

6.3.6 Gestión de Vulnerabilidades:

• **Escaneo de vulnerabilidades:** Identificar las debilidades en los sistemas y aplicaciones.

• **Gestión de parches:** Aplicar parches de seguridad de manera oportuna.

• **Priorización de vulnerabilidades:** Enfocarse en las vulnerabilidades que representan un mayor riesgo.

6.3.7 Seguridad de la Aplicación:

• **Desarrollo seguro:** Incorporar prácticas de desarrollo seguro en todo el ciclo de vida del software.

• **Pruebas de penetración:** Evaluar la seguridad de las aplicaciones antes de su despliegue.

• **WAF (Web Application Firewall):** Proteger las aplicaciones web de ataques comunes.

6.3.8 Respaldo y Recuperación de Datos:

• **Respaldos regulares:** Realizar copias de seguridad de los datos de forma periódica.

• **Pruebas de recuperación:** Verificar la integridad de los respaldos y la capacidad de restaurar los datos.

6.3.9 Seguridad de la Red:

• **Firewalls:** Filtrar el tráfico de red para bloquear el acceso no autorizado.

• **VPN/ZTNA:** Crear conexiones seguras y encriptadas para el acceso remoto.

• **Segmentación de redes:** Dividir la red en zonas de seguridad para limitar el impacto de posibles brechas.

6.3.10 Controles Físicos:

- **Control de acceso:** Limitar el acceso físico a las instalaciones y equipos.

- **Vigilancia:** Implementar sistemas de vigilancia para detectar actividades sospechosas.

- **Respaldo físico:** Proteger los equipos y la infraestructura frente a desastres naturales y otros eventos.

En general, es imperioso fomentar una cultura de seguridad en toda la organización para el éxito de cualquier programa de seguridad. La evolución constante de las amenazas implica mantener un enfoque proactivo para estar al tanto de las últimas tendencias en ciberseguridad. Por lo cual, los controles de seguridad deben adaptarse a las necesidades específicas de cada organización.

→ 7. FACTOR D.5.3: CALIDAD DEL SOFTWARE

→ 7.1. CONTEXTO

En el presente capítulo se aborda la calidad del software en los sectores público y privado de Chile, con un enfoque especial en la implementación de políticas y procesos de actualización y mantenimiento basados en evaluaciones de riesgo. También se hace hincapié en la importancia de adoptar estándares internacionales, como los asociados a la familia de las ISO/IEC 25000 para la calidad del software y la ISO/IEC 27000 para la seguridad de la información, a fin de garantizar que las soluciones tecnológicas desarrolladas cumplan con los criterios de seguridad, funcionalidad, eficiencia y mantenibilidad. La discusión proviene de un foro especializado que reunió a expertos del sector público, privado y académico, quienes compartieron sus puntos de vista sobre los desafíos y oportunidades relacionados con la mejora de la calidad del software.

→ 7.2. HALLAZGOS

7.2.1 Desafíos en la calidad del software en los sectores público y privado en Chile

- En el **sector público,** uno de los desafíos más relevantes es la integración de **sistemas heredados** con nuevas tecnologías, lo que genera dificultades para la implementación de soluciones modernas. Además, la **falta de estandarización** en las metodologías de desarrollo y la **resistencia al cambio** son obstáculos significativos. Otro reto importante es la existencia de **limitaciones presupuestarias y políticas,** lo que dificulta la implementación de procesos robustos de aseguramiento de calidad.

- La principal presión en el **sector privado** viene de la necesidad de reducir los **tiempos de entrega** (time-to-market), lo cual puede comprometer la calidad del software. También se identifica la **escasez de profesionales calificados** para realizar pruebas y procesos de aseguramiento de calidad, lo que afecta la capacidad de las empresas para garantizar productos de alta calidad.

• Uno de los principales desafíos en Chile, también, respecto a la calidad del software es la escasez de profesionales capacitados en metodologías avanzadas y herramientas específicas. Además, la falta de un marco regulatorio robusto ha limitado la adopción de estándares internacionales. Para abordar esta problemática, se recomienda fomentar la **capacitación continua** en metodologías de calidad del software y herramientas avanzadas como TDD (Test Driven Development), BDD (Behavior Driven Development) y CI/CD (Continuous Integration/Continuous Delivery), que permitan un enfoque proactivo y eficiente en el desarrollo de software.

• Otro desafío importante que se debe tener presente es sí las empresas que se dedican al desarrollo de software están considerando en sus procesos protocolos de seguridad robustos, que ayuden a evitar sean vulnerados una vez que estos se encuentran instalados y operando en las empresas. Con esto no solo nos referimos a sistemas de información de soporte al negocio, es decir, que son parte de las tecnologías de información, tales como los sistemas ERP para grandes, medianas y pequeñas empresas, sino también sistemas de apoyo al negocio como lo son las tecnologías de operación utilizados para controlar los equipos industriales y que se utilizan mayoritariamente en los sectores de fabricación, energía, medicina, minería, entre otros. En el caso de estos últimos (TO), muchos de estos sistemas (hardware y software) son diseñados para ser implementados en infraestructura crítica, como lo son los sistemas SCADA en el sector sanitario, por ejemplo. En este contexto, se recomienda que las empresas que desarrollan hardware y software incorporen protocolos de seguridad y calidad de software durante toda la etapa del ciclo de vida del desarrollo, así como también sensibilicen y eduquen a los usuarios en el buen uso del sistema evitando con ello un riesgo de ataque o intrusión.

7.2.2 Metodologías y herramientas utilizadas actualmente para asegurar la calidad del software en las organizaciones chilenas.

• Algunas organizaciones en Chile, tanto en el sector público como en el privado, utilizan metodologías ágiles como Scrum y Kanban, en combinación con prácticas DevOps, para integrar el aseguramiento de calidad en el ciclo de vida del desarrollo de software. Estas metodologías permiten una mayor flexibilidad en la gestión de requisitos y una entrega continua de valor.

• Las herramientas más utilizadas incluyen JIRA para la gestión de proyectos de desarrollo de software, Selenium y Appium para pruebas automatizadas, y SonarQube para el análisis de código estático. Estas herramientas son fundamentales para garantizar la calidad y la seguridad en cada etapa del ciclo de desarrollo, así como también para garantizar una mayor eficiencia, reducir errores humanos y mejorar la calidad del software desde las primeras etapas del desarrollo.

• El uso de metodologías ágiles y herramientas de automatización ha demostrado ser efectivo para mejorar la calidad del software. Sin embargo, aún existe una implementación desigual en sectores clave.

7.2.3 Gestión de requisitos funcionales en proyectos de software.

• En parte del **sector público,** prevalece el uso de metodologías tradicionales como waterfall, donde los requisitos funcionales se definen al inicio del proyecto y, una vez aprobados, es difícil modificarlos durante el ciclo de vida del desarrollo. Este enfoque, aunque efectivo en proyectos bien definidos, carece de la flexibilidad necesaria para adaptarse a cambios o mejoras surgidas durante el proceso. Además, la creación de documentos de especificación detallada podría ser obligatoria lo cual puede ralentizar el proceso y dificultar la gestión de cambios.

• Una limitación significativa en este sector es la resistencia al cambio y la falta de estandarización en las metodologías de desarrollo, lo que dificulta la adopción de prácticas más ágiles y flexibles. Para mitigar estos desafíos, es crucial fomentar la adopción de estas prácticas y la colaboración estrecha con los usuarios finales a lo largo de todo el proyecto.

• Es esencial que el sector público comience a adoptar métodos híbridos que combinen lo mejor de ambos enfoques. Esto incluiría la incorporación de demos periódicas y la utilización de User Stories para mejorar la interacción con los usuarios. Además, es crucial establecer un proceso de validación continua que permita una mayor flexibilidad en la gestión de cambios.

• La adopción de herramientas de gestión de requisitos como JIRA o Confluence puede facilitar la trazabilidad y el manejo de cambios para garantizar que los requisitos evolucionen con las necesidades del proyecto y se mantenga un alto nivel de calidad en el desarrollo de software.

• En algunas empresas del sector privado predominan las metodologías ágiles como Scrum y Kanban, que permiten una gestión de requisitos más dinámica, los que son refinados de manera continua a lo largo del proyecto, con la participación activa de los usuarios finales en cada iteración. Esta retroalimentación constante asegura que los cambios puedan ser implementados de forma rápida, lo que mejora la adaptabilidad y aumenta la satisfacción del cliente.

• Un aspecto clave es la participación de los usuarios finales en la definición de los requisitos, lo cual se facilita a través de User Stories y Sprint Reviews, prácticas comunes en metodologías ágiles. Estas técnicas permiten que los requisitos funcionales se alineen mejor con las necesidades reales del usuario final, reduciendo el riesgo de malentendidos o entregas incompletas.

7.2.4 Evaluación de riesgos.

• En parte del sector público, antes de realizar actualizaciones de software, se llevan a cabo **análisis de impacto detallados** que aseguran la continuidad de los servicios esenciales, especialmente en áreas críticas como salud, educación y sector financiero. Estas evaluaciones incluyen **matrices de impacto-probabilidad** que permiten identificar los riesgos más significativos y aplicar estrategias de mitigación adecuadas, tales como realizar pruebas en entornos de staging antes de la actualización en entornos de producción.

• Por otro lado, en el sector privado, la presión por reducir tiempos de inactividad impulsa el uso de **pruebas automatizadas y CI/CD** (Integración Continua/Despliegue Continuo) que permiten lanzar actualizaciones con mayor rapidez y confiabilidad. Sin embargo, las pruebas de regresión y la validación de parches a menudo siguen siendo manuales, lo que genera cuellos de botella en el proceso de mantenimiento.

• La evaluación de riesgos es un elemento crítico en el ciclo de vida del software. Automatizar más fases del proceso de actualización, incluyendo pruebas de regresión y validación de parches mediante herramientas de CI/CD, permitirá reducir significativamente los tiempos de inactividad y minimizar los riesgos asociados con las actualizaciones.

7.2.5 Mantenimiento Proactivo.

En parte del sector público y del sector privado, la tendencia se está inclinando hacia un enfoque de **mantenimiento proactivo** que utiliza herramientas de monitoreo como **Nagios o Zabbix** para detectar fallos o degradaciones en el rendimiento antes de que afecten al usuario final. Estas herramientas permiten una gestión predictiva, lo que optimiza la capacidad de respuesta frente a incidentes.

El uso de **estrategias de alta disponibilidad** (HA), como la replicación de bases de datos y el balanceo de carga, es esencial para reducir los tiempos de inactividad y garantizar la resiliencia frente a fallos. Además, la **automatización del ciclo de despliegue** a través de herramientas como **Jenkins y Ansible** reduce significativamente la posibilidad de errores humanos durante las actualizaciones.

Para optimizar el proceso de actualización y mantenimiento en Chile, es fundamental:

- **Automatizar más** fases del proceso de actualización, incluyendo pruebas de regresión y validación de parches, lo que puede lograrse mediante la integración de herramientas de CI/CD más robustas.

- **Formación continua** en técnicas avanzadas de evaluación de riesgos y en el uso de herramientas de monitoreo predictivo, asegurando que los equipos estén capacitados para realizar un mantenimiento proactivo y eficiente.

- **Metodologías de gestión de riesgos** basadas en estándares internacionales que apoyen en la evaluación del impacto de cada actualización y estrategias para minimizar interrupciones.

El mantenimiento proactivo es clave para garantizar la estabilidad y el rendimiento de los sistemas, por tanto, se recomienda implementar estrategias de alta disponibilidad (HA), como la replicación de bases de datos y el balanceo de carga, para minimizar interrupciones. Asimismo, integrar controles de seguridad en cada etapa del SDLC (Diseño, Desarrollo, Pruebas, Despliegue, Mantenimiento) fortaleciendo la resiliencia de los sistemas frente a posibles fallos.

7.2.6 Impacto de tecnologías emergentes como la inteligencia artificial y el Big Data en la calidad del software.

- La **IA y el Big Data** están revolucionando la calidad del software al permitir la **detección proactiva de defectos** y la optimización continua de procesos mediante **análisis predictivos y la automatización de pruebas.** Estas tecnologías ofrecen a las organizaciones la posibilidad de mejorar la precisión en las pruebas, personalizar soluciones de software y reducir los tiempos de respuesta frente a problemas técnicos.

7.2.7 Colaboración público-privada.

- Últimamente se han propiciado alianzas entre universidades, el gobierno y empresas privadas que buscan compartir buenas prácticas e impulsar la investigación y desarrollo en calidad de software y ciberseguridad.

→ 7.3. ACCIONES

7.3.1 Implementar Normativas y Estándares Internacionales.

• **Acción:** Adoptar y aplicar estándares internacionales, como la familia de la ISO/IEC 25000 sobre requisitos y evaluación de la calidad del sistema y del software y la familia de la ISO/IEC 27000 sobre seguridad de la información, junto con normativas locales relevantes, como la Ley de Ciberseguridad de Chile y las regulaciones específicas de protección de datos personales (Ley N° 19.628). Esto garantizará que la calidad y seguridad del software cumplan tanto con estándares globales como con los requerimientos específicos del entorno nacional, fortaleciendo la confianza de los usuarios y reduciendo riesgos asociados a vulnerabilidades en sistemas informáticos.

• **Resultado esperado:** Mejora en la conformidad con estándares internacionales, garantizando productos de software seguros y de calidad.

7.3.2 Automatización de pruebas y despliegue.

• **Acción:** Implementar herramientas de integración continua y automatización de pruebas, como Jenkins, Selenium y SonarQube, para asegurar una mayor eficiencia y reducción de errores humanos.

• **Resultado esperado:** Reducción en los tiempos de entrega y mejora en la calidad del software entregado, disminuyendo errores post-producción.

7.3.2 Fortalecer la gestión de riesgos.

• **Acción:** Desarrollar políticas de gestión de riesgos basadas en metodologías como PRINCE2 e ITIL, con análisis de impacto antes de cada actualización.

• **Resultado esperado:** Reducción de tiempos de inactividad y una mejor gestión de riesgos en las actualizaciones, asegurando la continuidad operativa.

7.3.3 Capacitación continua.

• **Acción:** Establecer programas de formación en metodologías de calidad del software, como TDD (Test-Driven Development) y BDD (Behavior-Driven Development), además de herramientas de CI/CD.

• **Resultado esperado:** Equipos de desarrollo más capacitados y actualizados en buenas prácticas de calidad y ciberseguridad.

7.3.4 Monitoreo y mantenimiento proactivo

• **Acción:** Utilizar herramientas como Nagios o Zabbix para monitoreo continuo y asegurar un mantenimiento proactivo basado en evaluaciones de riesgo.

• **Resultado esperado:** Menor interrupción del servicio y tiempos de inactividad, mejorando la seguridad y rendimiento del software.

7.3.5 Gestión del Software

• **Acción 1:** Implementar validación de entradas en el lado del servidor y cliente. Resultado esperado: Reducción de vulnerabilidades.

• **Acción 2:** Asegurar configuraciones seguras en todas las etapas del ciclo de vida del desarrollo del Software.

• **Resultado esperado:** Reducción de vulnerabilidades.

• **Acción 3:** Integrar controles de seguridad en cada fase del SDLC (Diseño, Desarrollo, Pruebas, Despliegue, Mantenimiento).

• **Resultado esperado:** Reducción de vulnerabilidades.

7.3.6 Indicadores de madurez y calidad.

• **Acción:** Desarrollar un marco de indicadores de madurez, utilizando métricas como la cobertura de pruebas automatizadas y el número de defectos encontrados.

• **Resultado esperado:** Evaluación objetiva del rendimiento de los equipos de desarrollo, permitiendo identificar áreas de mejora y optimizar procesos.

7.3.7 Fomentar la colaboración público-privada.

• **Acción:** Promover alianzas estratégicas entre los sectores público, privado y académico para compartir conocimientos y mejorar las políticas de calidad del software y ciberseguridad.

• **Resultado esperado:** Mayor coherencia en las prácticas de calidad a nivel nacional, fomentando la innovación y mejora continua en el desarrollo de software.

→ Reflexiones Generales

La calidad del software y la ciberseguridad son fundamentales para garantizar la eficiencia operativa, seguridad y continuidad de servicios en las organizaciones, tanto en el sector público como en el privado. A través de la adopción de normativas internacionales como la familia de las ISO/IEC 25.000 sobre requisitos y evaluación de la calidad del sistema y del software e ISO/IEC 27.000 sobre seguridad de la información, las organizaciones pueden asegurar que sus productos cumplen con altos estándares de calidad y seguridad.

El uso de tecnologías emergentes como la inteligencia artificial y el Big Data están transformando el desarrollo de software, proporcionando herramientas que permiten una mayor precisión en la detección de errores y la mejora continua en los procesos. A su vez, la implementación de pruebas automatizadas y monitoreo proactivo permite identificar y corregir problemas antes de que afecten a los usuarios finales, minimizando tiempos de inactividad y mejorando la satisfacción del cliente.

Un aspecto crucial para garantizar el éxito a largo plazo es la capacitación continua de los equipos de desarrollo en metodologías ágiles, buenas prácticas de ciberseguridad y herramientas avanzadas de CI/CD. Esto asegura que las organizaciones estén preparadas para enfrentar los desafíos de un entorno tecnológico en constante cambio.

Finalmente, las colaboraciones público-privadas son clave para fomentar la innovación y compartir mejores prácticas. La creación de alianzas estratégicas entre el gobierno, el sector privado y el ámbito académico pueden impulsar la mejora de las políticas de calidad del software y ciberseguridad en Chile, posicionando al país como un referente en la adopción de tecnologías emergentes y en el aseguramiento de la calidad del software.

→ 8. FACTOR D.5.4: COMUNICACIONES E INTERNET RESILIENCIA DE LA INFRAESTRUCTURA

→ 8.1. CONTEXTO

Este capítulo analiza la resiliencia de la infraestructura de Internet en Chile, enfocándose en cómo el gobierno, el sector público y privado protegen los servicios críticos. Examina la implementación de procesos de seguridad, incluyendo gestión de riesgos, detección de intrusiones y respuesta a incidentes. También se evalúan los mecanismos para realizar evaluaciones de riesgos y monitorear la resiliencia de la red, considerando la redundancia, diversidad de rutas y recuperación ante desastres.

Se destaca la importancia de adoptar estándares internacionales como *NIST Cybersecurity Framework, CIS Controls, ISO/IEC 27032 e ISO/IEC 27001* para asegurar una infraestructura robusta y resistente a ciberataques. Se exploran las implicaciones de la dependencia de proveedores externos y el control gubernamental sobre la infraestructura crítica.

La discusión se basa en un foro con expertos que analizaron los desafíos y oportunidades para fortalecer la resiliencia de Internet en Chile, incluyendo la inversión en infraestructura segura, el desarrollo de capacidades nacionales y la cooperación público-privada.

→ 8.2. HALLAZGOS

8.2.1 Desafíos de la Resiliencia de La Infraestructura Crítica

• El panorama de amenazas cibernéticas está en constante evolución, lo que dificulta la protección contra todos los ataques. Las organizaciones deben ser capaces de adaptarse rápidamente a las nuevas amenazas y actualizar sus medidas de seguridad de forma regular. En 2019, la Base de Datos Nacional de Vulnerabilidades (NVD) del Instituto Nacional de Estándares y Tecnologías (NIST) registró más de 17.000 nuevas vulnerabilidades de software, mientras que el año 2024 registró cerca de 40.000 de ellas. Por lo tanto, el crecimiento porcentual de las vulnerabilidades del NVD entre 2019 y 2024 es aproximadamente 131.16%. Esto significa que el número de vulnerabilidades registradas en el NVD aumentó en más del doble en este período.

• En muchos casos, las organizaciones no son plenamente conscientes de los riesgos cibernéticos que enfrentan o no tienen el conocimiento necesario para protegerse adecuadamente. Esto puede llevar a una falta de inversión en ciberseguridad y a la implementación de medidas inadecuadas. En 2023, el Informe de Riesgos Globales del Foro Económico Mundial clasificó los ciberataques como una de las principales amenazas para la economía global, en contraste ese mismo año un informe de IBM Ponemon Institute reveló que el **68%** de las organizaciones no creen que estén preparadas para responder a un ciberataque.

• La ciberseguridad puede ser costosa, y muchas organizaciones, especialmente en el sector público, pueden tener recursos limitados para invertir en ella. Esto puede dificultar la adquisición de tecnologías, la contratación de personal capacitado y la implementación de programas de capacitación.

• Un informe de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) de 2023 destaca que la inversión en ciberseguridad en el sector público sigue siendo insuficiente en muchos países. En el mismo periodo, el Estudio de la Fuerza Laboral de Ciberseguridad de ISC2 estimó una brecha de **3,4 millones** de profesionales de ciberseguridad en todo el mundo. Esta brecha es especialmente pronunciada en el sector público, donde las organizaciones a menudo luchan por competir con los salarios y beneficios ofrecidos por el sector privado.

• La cooperación entre las organizaciones es esencial para la resiliencia de la infraestructura crítica. Sin embargo, muchas organizaciones no comparten información sobre amenazas o no colaboran en la respuesta a incidentes. Esto puede dificultar la detección y mitigación de ataques. Un informe de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) de 2020 encontró que el 65% de las organizaciones no comparten información sobre ciberamenazas con otras organizaciones.

8.2.2 Metodologías Orientadas a la Resiliencia de La Infraestructura Crítica

• El aseguramiento de la resiliencia de la infraestructura crítica puede ser vista como un proceso que está sujeto a un ciclo de mejora continua. El modelo PDCA de Deming es un ciclo iterativo de cuatro etapas que se utiliza para la mejora continua de procesos, y si bien es una herramienta valiosa para la gestión de la calidad, es ampliamente utilizado en la gestión de riesgos y la continuidad del negocio. Se utiliza para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente los sistemas de gestión de continuidad del negocio. El estándar internacional **ISO/IEC 22301** para la gestión de la continuidad del negocio promueve el uso del ciclo PDCA para la mejora continua de los sistemas de gestión de continuidad del negocio.

• Considerando esta cualidad iterativa, que es propia del proceso de ciberseguridad, es conveniente destacar la importancia de adoptar estándares internacionales, como el Marco de Ciberseguridad del NIST (NIST, 2018), para guiar la implementación de medidas de seguridad, ya que diversos controles estratégicos ya se encuentran estandarizados como podemos identificar en ISO/IEC 27.002 (ISO/IEC, 2022) y Controles CIS (CIS, 2021). Aunque no es un estándar certificable como la ISO 27001, la ISO 27002 sirve como un complemento que ayuda a las organizaciones a implementar los controles de seguridad necesarios para cumplir con la ISO 27001. A su vez, el objetivo de los controles CIS es ayudar a las organizaciones a reducir su riesgo de ciberataques mediante la implementación de un conjunto de medidas de seguridad probadas y eficaces. Un estudio de PwC de 2022 encontró que el 70% de las organizaciones utilizan el Marco de Ciberseguridad del NIST para guiar sus esfuerzos de ciberseguridad.

8.2.3 Requisitos Mínimos en la Resiliencia de La Infraestructura Crítica

• Se debe contar con un proceso para identificar y clasificar los activos de infraestructura crítica, incluyendo los sistemas, redes y datos que son esenciales para la operación, ya sea de servicios públicos o privados. Si los activos críticos están identificados, será posible evaluar el riesgo periódicamente considerando las amenazas y vulnerabilidades propias de cada organización y que tengan el potencial de afectar la infraestructura crítica. Si bien,el problema de las tecnologías en las sombras **(Shadow IT)** parece inofensivo, plantea serios riesgos para las organizaciones ya que el uso de hardware o software dentro de una organización sin el conocimiento o aprobación explícita del departamento de TI puede permitir el movimiento lateral de los atacantes inadvertidamente.

• La gestión de riesgo se vería incompleta sin la implementación de controles de seguridad técnicos, físicos y administrativos para proteger la infraestructura crítica de ataques. El estándar internacional ISO/IEC 27001 requiere que las organizaciones implementen controles de seguridad para gestionar los riesgos de seguridad de la información. La certificación ISO 27001 es cada vez más popular, ya que las organizaciones reconocen la importancia de un Sistema de Gestión de Seguridad de la Información (SGSI) sólido para proteger sus activos de información.

• En la dimensión de continuidad de la operación, se deben establecer planes que garanticen que los servicios esenciales puedan continuar funcionando en caso de un incidente cibernético, así como también, planes para restaurar la infraestructura crítica. Un informe de Gartner de 2023 encontró que el 65% de las organizaciones han experimentado una interrupción significativa en sus operaciones en los últimos dos años.

• Lo anterior, implica monitorear los sistemas críticos en busca de actividad maliciosa, y así responder y mitigar los incidentes de seguridad basándonos en un plan de respuesta a incidentes. Estos esfuerzos deben ser comprobados a través de ejercicios o pruebas. Un estudio del Ponemon Institute de 2022 reveló que el costo promedio de una interrupción del centro de datos es de USD$9,000 por minuto.

8.2.4 Tecnologías Emergentes en la Resiliencia de La Infraestructura Crítica

• Actualmente, la inteligencia artificial presenta un caso paradójico, permitiendo detectar patrones anómalos que podrían indicar un ciberataque tras analizar grandes volúmenes de datos de tráfico de red. Sin embargo, también puede convertirse en una amenaza con el potencial de ser usada para desarrollar un ataque u ofensiva. En 2021, una encuesta de ISC2 encontró que el 43% de los profesionales de ciberseguridad creen que la IA será utilizada por los ciberdelincuentes para llevar a cabo ataques más sofisticados.

• De manera semejante, la tecnología de encadenamiento de bloques, Blockchain, también tiene el potencial de contribuir en resguardar la integridad de la cadena de suministro de software y hardware, reduciendo el riesgo de que se introduzcan componentes vulnerables o maliciosos en la infraestructura crítica. Sin embargo, algoritmos de consenso que hacen uso intensivo de la capacidad computacional, y así del suministro eléctrico presentan un escenario problemático de escalamiento. En 2021, un estudio de la Universidad de Cambridge estimó que la red Bitcoin consume aproximadamente 121 teravatios-hora de electricidad al año, lo que es comparable al consumo de energía de países como Argentina.

8.2.5 Relación Público y Privada en la Resiliencia de La Infraestructura Crítica

• La infraestructura crítica a menudo es propiedad y está operada por entidades privadas, pero su disrupción tiene un impacto público masivo. El sector público aporta marcos regulatorios, financiamiento y conocimiento del interés público, mientras que el privado posee la experiencia técnica, la innovación y la gestión de la infraestructura. De este modo, ningún sector puede abordar este desafío por sí solo. Las amenazas son cada vez más sofisticadas y requieren de una respuesta coordinada que involucre a ambos sectores. Un informe del Foro Económico Mundial de 2023 destaca la importancia de la colaboración público-privada para la protección de la infraestructura crítica.

→ 8.3. ACCIONES

8.3.1 Intercambiar información.

• **Acción:** Compartir información sobre amenazas, vulnerabilidades y mejores prácticas es fundamental. Esto incluye la creación de centros de intercambio de información y la promoción de la transparencia. La detección temprana y la contención rápida son cruciales para minimizar el impacto de un incidente de seguridad.

• **Resultado esperado:** Mejorar el tiempo medio de detección de incidentes y brechas. De acuerdo a Verizon en su reporte DBIR (2023), una corporación tarda entre 16 y 728 días en detectar una brecha, siendo la mediana de tiempo 21 días. Además, se espera mejorar el tiempo de contención, según Verizon DBIR (2023), la contención más rápida ocurre en el orden de minutos y sólo el 1% de las corporaciones responden con esta prontitud, mientras que la contención más lenta ocurre en el orden de meses o incluso años situación que le ha ocurrido a cerca del 15% de las corporaciones analizadas. El tiempo medio de recuperación se estima en 28 días.

• **Acción:** Fomentar la investigación y el desarrollo de nuevas tecnologías y soluciones para la resiliencia de la infraestructura crítica. Un ejemplo significativo es el desarrollo de la interoperabilidad entre naciones que colabora en el acceso y portabilidad de los datos protegiendo su privacidad (Comisión Europea, 2017). Actualmente, instituciones como ISO, ITU y W3C han expandido sus estándares para incluir la interoperabilidad, así como tendencias que promueven la apertura de interfaces API (Waher, 2024), microservicios, e incluso la misma tecnología Blockchain puede facilitar la interoperabilidad y la confianza en el intercambio de datos.

• **Resultado esperado:** Aumento de la inversión en I+D, el porcentaje del PIB dedicado a I+D sigue siendo bajo en comparación con otros países de la OCDE. El promedio de la OCDE es de **2,75% del PIB,** lo que coloca a Chile en una posición rezagada considerando que su inversión en I+D se ha mantenido estable en la última década, con leves fluctuaciones entre **0.33% y 0.39%.**

8.3.2 Desarrollo de Estándares y Financiamiento.

• **Acción:** El sector público puede establecer estándares de seguridad y resiliencia, mientras que el privado puede contribuir con su experiencia para que sean prácticos y efectivos.

• **Resultado esperado:** Desarrollo de un ecosistema sostenible que permita la colaboración público, privada y académica para acelerar los procesos de investigación aplicada en ciberseguridad. Impulsar un enfoque de diseño seguro incentivado o financiado por el sector público para que las empresas y comunidades académicas inviertan en medidas innovadoras de resiliencia en infraestructura crítica.

8.3.3 Planificación y Ejercicios Conjuntos.

• **Acción:** Realizar simulacros y ejercicios conjuntos permite a ambos sectores prepararse para responder a incidentes de manera coordinada.

• **Resultado esperado:** La colaboración público-privada es esencial para fortalecer la resiliencia de la infraestructura crítica. Al trabajar juntos, ambos sectores pueden proteger mejor los servicios esenciales de los que dependen nuestras sociedades y economías. Existen ejemplos concretos, como la iniciativa sobre ciber resiliencia en la electricidad, y grupos operativos entre la Unión Europea y la OTAN centrado en la resiliencia en energía, transporte, el sector digital y espacio (Comisión Europea, 2023).

Chile necesita un enfoque integral que combine la adopción de estándares, la cooperación público-privada y la inversión en tecnologías para garantizar la resiliencia de su infraestructura de Internet y proteger sus servicios esenciales.

El gobierno, el sector público y privado deben colaborar para afrontar los desafíos de un panorama de amenazas en constante evolución. Los desafíos identificados se relacionan con un grado de conciencia y conocimiento de ciberseguridad aún limitados, así como de recursos insuficientes para invertir en protección, además de la escasa cooperación entre organizaciones. De este modo, recomendamos adoptar estándares internacionales e implementar procesos de mejora continua. Un esfuerzo que debe sustentarse en un esfuerzo previo por identificar y evaluar el riesgo de los activos críticos, para que la implementación de controles de seguridad y planes de recuperación sean coherentes. Y también, de un monitoreo y respuesta oportuna ante incidentes.

Por último, las tecnologías emergentes como la inteligencia artificial y Blockchain ofrecen oportunidades y desafíos para la ciberseguridad, que nos interpelan a colaborar entre sectores público y privado. Es gravitante compartir información sobre amenazas y mejores prácticas, desarrollar estándares y financiar la investigación de la interoperabilidad entre naciones. Así como también, es importante la realización de simulacros conjuntos entre sectores para fortalecer la resiliencia de la infraestructura crítica.

→ 9. FACTOR D.5.5: MERCADO DE CIBERSEGURIDAD

→ 9.1. CONTEXTO

El mercado de la ciberseguridad en Chile ha experimentado un crecimiento significativo en los últimos años, impulsado por el aumento de las amenazas cibernéticas y la creciente dependencia de las tecnologías digitales en el sector empresarial. Sin embargo, aún existen brechas y desafíos que deben ser abordados para fortalecer la seguridad cibernética a nivel nacional.

A nivel global, el desempeño de los países sudamericanos en los índices Global Cybersecurity Index GCI (ITU, 2015) y el National Cyber Security Index NCSI (EGA, 2018) históricamente ha mostrado una tendencia de mejora, pero siguen teniendo deficiencias en áreas clave como la capacidad de cooperación internacional y respuesta técnica a incidentes cibernéticos. En la última edición del GCI (2021) se puede visualizar a Brasil liderando la región, situado en el puesto dieciocho a nivel mundial y a Uruguay y Chile complementando el top tres de Sudamérica en el ranking global. Por el lado del índice NCSI, Brasil, Uruguay y Chile destacan históricamente en las mediciones y, en el caso más reciente (2024), Chile escaló treinta puestos en el ranking mundial de ciberseguridad, posicionándose en el lugar número veinticinco a nivel global y segundo en América Latina. Un mejor ranking implica mayor inversión y desarrollo del mercado.

→ 9.2. HALLAZGOS

A continuación, se presenta una síntesis del estado del arte en Chile sobre el mercado empresarial de la ciberseguridad, basada en diversas fuentes y estudios:

9.2.1 Crecimiento del mercado

El mercado de la ciberseguridad en Chile ha experimentado un crecimiento sostenido en los últimos años, impulsado principalmente mediante la demanda de soluciones de seguridad de la información por parte de las grandes empresas y el sector financiero.

9.2.2 Madurez del mercado

Si bien el mercado chileno ha mostrado un crecimiento sostenido, aún se encuentra en una etapa de madurez temprana en comparación con otros países de la región.

9.2.3 Principales actores

El mercado chileno está conformado por una variedad de actores, incluyendo empresas multinacionales, empresas nacionales e startups. Una muestra representativa de los principales proveedores de soluciones de ciberseguridad en Chile son:

Empresa	Enlace
acktib	**https://acktib.com/**
Base 4	**https://www.base4sec.com/#chile**
Cibernex	**https://cibernex.cl/ethical-hacking/**
Ciberlabs	**https://ciberlabs.cl**
CyberSecurity for all	**c4a.cl**
Corvus	**https://www.corvus.cl/**
Cronup	**https://www.cronup.com/contacto/**
Cyber-Protection	**https://www.cyber-protection.cl/**
Cybertrust	**https://www.cybertrust.cl/**
DevelR0X	**https://develrox.com/es/**
Dreamlab	**https://dreamlab.net/es/servicios/**
Entelgy	**https://www.entelgy.com/**
hackmetrix	**https://www.hackmetrix.com/ethical-hacking**
iHack	**https://ihack.red/**
Infinity spa	**https://infinityspa.cl/**
infocorp	**https://infocorp.cl/ethical-hacking/**
InsideSecurity	**https://www.insidesecurity.cl/**
Helpsystem	**Core Impact * hacking infraestructura ****
ITBOX ltda	**https://itbox.cl/**

Empresa	Enlace
Kepler	**https://kepler.cl/contacto/**
Makros	**https://makros.cl/solutions/ethical-hacking**
Neuronet	**https://neuronet.cl/**
Nivel 4	**https://www.nivel4.com**
Novared	**https://www.novared.net/**
Oznet	**https://www.oznet.cl/**
Pentest	**https://www.pentest.cl/cotizar/**
TrustTech	**https://www.trusttech.cl/**
Unitti	**https://www.unitti.com/**
Tecnovan	**https://www.tecnovan.com/**
Isecurity	**https://isecurityqa.com/**

Figura: Tabla 1

9.2.4 Resultados Encuestas

Se realizó un periodo breve de encuestas en el periodo Agosto a Septiembre para focalizar el esfuerzo del muestreo según consulta directa en la red social LinkedIn y los valores obtenidos por pregunta son los siguientes:

Figura 2: Resultados de Encuesta LinkedIn 1

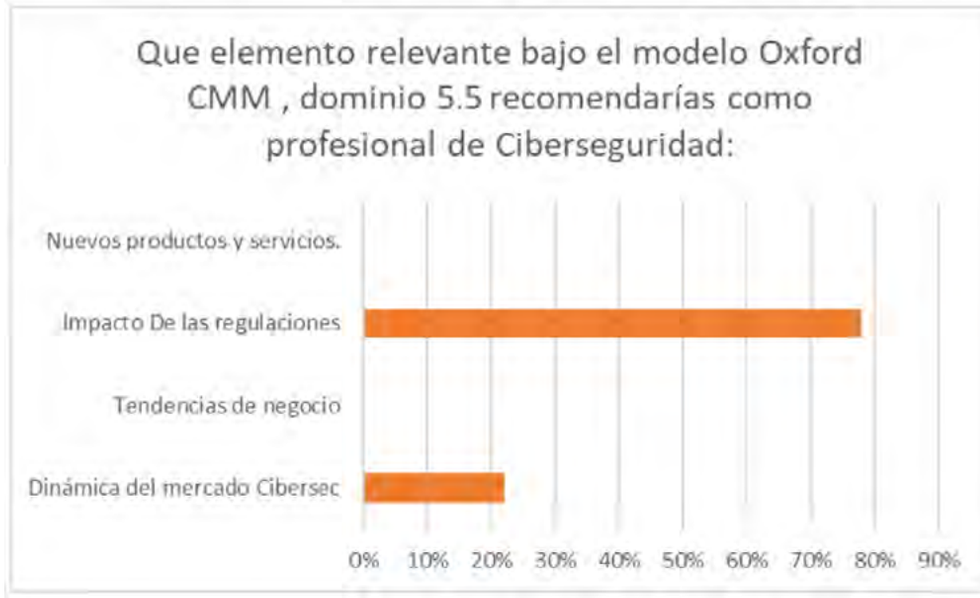


Figura 3: Resultados de Encuesta LinkedIn 2

→ 9.3. ACCIONES

Considerando la situación actual del mercado empresarial de la ciberseguridad en Chile, se propone adaptar la metodología Oxford, es decir, considerar una Metodología de Medición Adaptada a Chile, considerando los siguientes aspectos:

9.3.1 Indicadores específicos

• Incorporar indicadores que reflejen la realidad del mercado chileno, como el nivel de preocupación por de la Ley de Protección de Datos Personales, preparación para cumplimiento ley marco de Ciberseguridad, el impacto de los ciberataques en la economía nacional.

9.3.2 Fuentes de información

• Utilizar fuentes de información locales, como estudios realizados por universidades chilenas, cámaras empresariales y organismos gubernamentales.

9.3.3 Encuestas a actores del mundo Ciberseguridad

• Realizar encuestas específicas a un universo de personas con la participación de expertos en ciberseguridad, representantes de empresas y funcionarios gubernamentales para obtener una visión más detallada del mercado. Estas encuestas se realizan mediante la plataforma LinkedIn para aumentar el universo muestral.

En definitiva, el mercado de la ciberseguridad en Chile presenta un gran potencial de crecimiento, pero aún enfrenta desafíos importantes. Para fortalecer la seguridad cibernética a nivel nacional, es necesario promover la inversión en investigación y desarrollo, fomentar la formación de profesionales especializados, y establecer un marco regulatorio adecuado.

Se visualiza un mercado atomizado donde coexisten una variedad de oferentes, desde pequeñas empresas especializadas hasta proveedores de tamaño mediano. Este Nivel Medio de oferentes con oferta asimétrica es una característica común en mercados donde la especialización y los nichos son predominantes (hiper nicho). Tal oferta no responde de manera homogénea en base a solo beneficio esencial, primando la promoción por grados de madurez tanto comercial como de la especialización de los servicios y la complejidad de las tecnologías ofertadas. Es decir, en lugar de competir únicamente por el "beneficio esencial" (por ejemplo, el precio), los oferentes se enfocan en promover su grado de madurez y especialización, lo que les permite justificar precios más altos o atraer a clientes específicos.

En otros países se puede verificar el índice CAGR, como referencia el caso europeo, donde el tamaño del mercado europeo de ciberseguridad se estima en **USD 56,96** mil millones en **2024** y se espera que alcance los **USD 95,17** mil millones para **2029,** creciendo a una CAGR del **10,81%** durante el período de pronóstico (Mordor Intelligence, s. f.).

Para el caso nacional mediante el mismo indicador, la oferta no responde a una oferta base como en otros países en donde la diferenciación es por precio y áreas de especialización específicas (p.e. Tecnologías XDR, EDR, CS0C, MSP, entre otras).

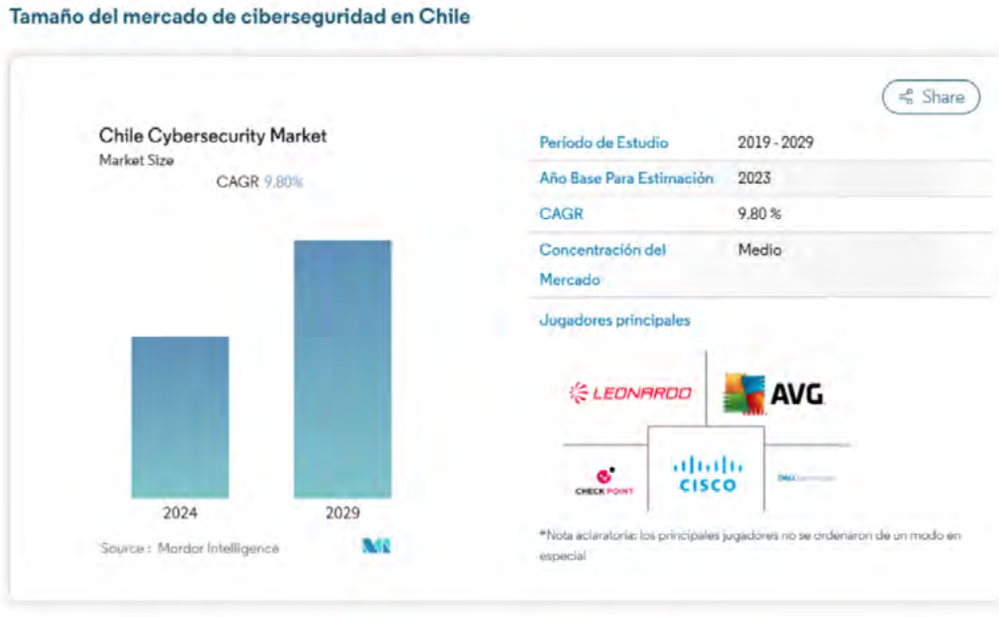


Figura 4 - Mercado de ciberseguridad en Chile - Mordor Intelligence.

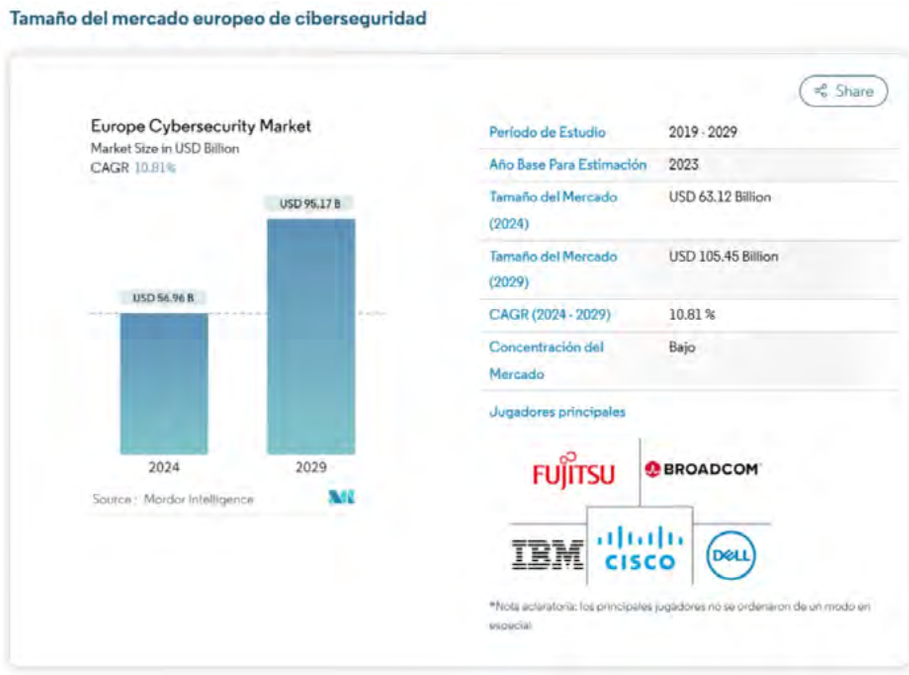


Figura 5 - Mercado de ciberseguridad en Europa - Mordor Intelligence.

Si bien, no se evidencia una diferencia significativa en el valor CAGR entre Europa y Chile, podemos obtener de referencia el siguiente indicador:

El mercado de ciberseguridad en Chile está experimentando un crecimiento significativo, impulsado por la necesidad de proteger sistemas y datos de ataques maliciosos. En 2024, se espera que el tamaño del mercado chileno alcance los **USD 348** millones, con una tasa de crecimiento anual compuesta (CAGR) del **10,3%** proyectada hasta **2032.** Este aumento está motivado por la creciente digitalización y la adopción de tecnologías emergentes como la inteligencia artificial y la computación en la nube. (Santiago, 2024).

Gráfico de referencia, Crecimiento de mercado proyectado:

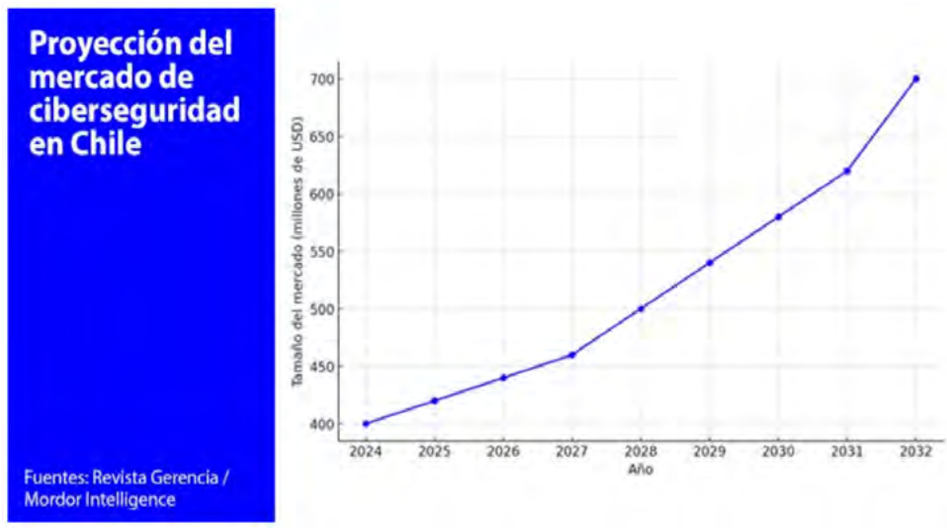


Figura 6 - Proyección del mercado de ciberseguridad en Chile - Revista Gerencia

Como equipo denotamos que, ante la aparición de la ley marco de ciberseguridad y el comienzo de su vigencia, se generó un aumento del interés sobre normas certificables tales como la ISO 27001:2022 *(ISO/IEC 27001:2022, n.d.)* y otros frameworks no certificables como NIST 2.0 *(The NIST Cybersecurity Framework (CSF) 2.0, 2023),* Cis Controls *(CIS Critical Security Controls Version 8, 2022),* entre otros.

→ 10. FACTOR D.5.6: DIVULGACIÓN RESPONSABLE

→ 10.1. CONTEXTO

Este factor examina el establecimiento de un marco de divulgación responsable para la recepción y difusión de información sobre vulnerabilidades en todos los sectores, y si existe la capacidad suficiente para revisar y actualizar continuamente dicho marco. Este factor se divide en dos aspectos.

10.1.1 Intercambio de información sobre vulnerabilidades:

Explora los mecanismos o canales existentes para el intercambio de información sobre los detalles técnicos de las vulnerabilidades entre las partes interesadas.

10.1.2 Políticas, procesos y legislación para la divulgación responsable de fallas de seguridad:

Examina la existencia de una política o marco de divulgación responsable en las organizaciones de los sectores público y privado, y el derecho a la protección legal de quienes divulgan fallas de seguridad. En Chile, el 12 de diciembre de 2023, se remitió para su trámite de promulgación el Proyecto que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. La iniciativa tiene por objeto establecer la institucionalidad indispensable para robustecer la ciberseguridad; ampliar y fortalecer el trabajo preventivo; formar una cultura pública en materia de seguridad digital; enfrentar las contingencias en el sector público y privado, y resguardar la seguridad de las personas en el ciberespacio. La norma fue publicada en el Diario Oficial el 8 de abril de 2024 bajo el número 21663. Entre otras materias, crea la Agencia Nacional de Ciberseguridad (ANCI), que tendrá facultades para fiscalizar, regular y sancionar a instituciones prestadoras de servicios esenciales, sean públicas o privadas. Definirá los operadores de importancia vital (OIV) y dictará protocolos, estándares e instrucciones generales y particulares, de carácter obligatorio, para implementar la Ley Marco. La ANCI también asesorará al Presidente en la elaboración de políticas, planes y programas de acción. Adicionalmente, la ANCI administrará el Registro Nacional de Incidentes (RNI), requerirá antecedentes para prevenir su ocurrencia y promoverá la educación en ciberseguridad.

→ 10.2. HALLAZGOS

La limitada participación en el foro de ciberseguridad ha afectado significativamente la calidad del análisis y la toma de decisiones respecto al subdominio 5.6 Divulgación responsable. La falta de aportes diversos y de múltiples perspectivas impide obtener una visión completa de los desafíos actuales en la materia. Sin una cantidad representativa de opiniones y experiencias, resulta difícil validar las tendencias observadas o identificar riesgos emergentes con precisión. Además, se pierde la oportunidad de generar un debate constructivo que podría ofrecer soluciones innovadoras y efectivas. Esta situación nos deja con información incompleta y, en consecuencia, no es posible llegar a conclusiones certeras o bien fundamentadas sobre los temas tratados.

→ 10.3. ACCIONES

Para abordar esta situación compleja, se propone realizar encuestas específicas a un universo de personas con la participación de expertos en ciberseguridad, representantes del sector privado y público, para obtener conclusiones que aporten a estos dos aspectos:

10.3.1 Intercambio de información sobre vulnerabilidades.

Crear un mecanismo que permita compartir de manera ágil y segura información sobre vulnerabilidades, para mejorar la capacidad de todos los actores para protegerse ante las ciberamenazas.

10.3.2 Políticas, procesos y legislación para la divulgación responsable de fallas de seguridad.

Establecer un ecosistema de ciberseguridad más seguro y resiliente, donde las vulnerabilidades se gestionen de manera efectiva y responsable.

→ 11. CONVERGENCIA DE ACCIONES CON IMPACTO NACIONAL

Para abordar los desafíos y aprovechar las oportunidades en ciberseguridad en Chile, se propone un conjunto de acciones unificadas que maximicen su impacto. Esta integración de acciones están dirigidas a la política pública, para fomentar la colaboración y la sinergia de los sectores:

→ 11.1 SÍNTESIS DE LOS DESAFÍOS Y OPORTUNIDADES

Actualmente, la clasificación de las empresas por tamaño se basa principalmente en sus ventas anuales, y a modo de estimación podemos considerar que las microempresas representan el 70% de las empresas en Chile, seguidas de las pequeñas y medianas empresas que constituyen cerca del 25%. De este modo, las grandes empresas representan un porcentaje no superior al 2%. De este modo, enfrentamos un escenario evidente de disparidad en la madurez de la ciberseguridad entre sectores, con sectores como el comercio minorista y servicios de salud primaria con menores niveles de protección. Si bien, la cantidad de empresas certificadas ISO 27001 en Chile probablemente ha ido en aumento en los últimos años debido a la creciente importancia de la ciberseguridad y la protección de datos, aún el número estimado no supera las 200 empresas. La gestión de riesgos en la cadena de suministro, especialmente en las pequeñas y medianas empresas es débil, es decir, el marco regulatorio es insuficiente y debe reglamentar de manera clara el cumplimiento en los distintos sectores. Los sistemas heredados y su integración con las tecnologías emergentes son desafiantes para distintos sectores. Se necesitan estándares sectoriales, así como estímulo a la capacitación, para enfrentar la problemática de escasez de profesionales calificados en pruebas y aseguramiento de calidad. Más aún, la resiliencia de internet no sólo implica mayor inversión, es también un desafío a la cooperación entre organizaciones para que los incidentes y brechas de seguridad sean apropiadamente notificados para el entendimiento común. Aún la conciencia y conocimiento de ciberseguridad es limitado. Esto se refleja en un mercado de ciberseguridad en una etapa temprana de madurez en comparación con otros países de la región, caracterizado por un número limitado con oferta asimétrica.

Por otro lado, la nueva institucionalidad de la Ley N° 21.663 Marco de Ciberseguridad es un impulso transversal en Chile. Repercute en la oferta de programas de formación en ciberseguridad para distintos profesionales especializados en la disciplina.

El marco regulatorio fomenta la colaboración entre el sector público y privado para fortalecer la ciberseguridad en la cadena de suministro. Se observa que distintas organizaciones que manejan información sensible o crítica, como datos personales, información financiera, propiedad intelectual, entre otras, se ven beneficiadas de la certificación ISO 27001. La certificación no solo ayuda a proteger la información, sino que también mejora la imagen de la organización, aumenta la confianza de los clientes y puede ser un requisito para cumplir con regulaciones y leyes de protección de datos. Adicionalmente, se promueve la inversión progresiva en investigación y desarrollo tanto de nuevas tecnologías como de nuevo conocimiento. A su vez, el ecosistema de ciberseguridad permite impulsar un enfoque de diseño seguro incentivado o financiado por el sector público. Todo esto se ve potenciado con las alianzas estratégicas entre los sectores público, privado y académico, lo que de manera sostenida nos puede conducir a la adaptación metodológica a la realidad chilena.

→ 11.2 CONVERGENCIA DE ACCIONES DIRIGIDAS A LA POLÍTICA PÚBLICA

El marco regulatorio debe incluir la convergencia de la tecnología empresarial y la tecnología industrial (TI/TO). Considerar el nivel de madurez de cada sector y adaptar la regulación a sus necesidades. De paso promover la creación de incentivos para que las empresas inviertan en ciberseguridad. El intercambio de información sobre amenazas, vulnerabilidades y mejores prácticas se torna indispensable para una implementación efectiva de la Ley. Es necesario apoyar la creación de CSIRT's sectoriales para la respuesta coordinada a incidentes. Así como también, estimular el financiamiento en la investigación y desarrollo de nuevas tecnologías y soluciones de ciberseguridad. Lo anterior, acompañado de campañas de concientización pública sobre ciberseguridad, así como, incorporar programas a todos los niveles educativos en pos de la formación de capacidades en Chile.

→ 11.3 PRIORIZACIÓN DE ACCIONES

Para fortalecer la ciberseguridad en Chile a través de la acción gubernamental se proponen tres ejes principales: El Fortalecimiento del marco regulatorio, el Fomento de la colaboración público y privada, y la Inversión en educación y concientización.

El fortalecimiento del marco regulatorio implica considerar las necesidades de cada sector, incluyendo la integración de tecnologías empresariales e industriales (TI/TO), así como proteger la infraestructura crítica.

La colaboración público y privada requiere crear plataformas de intercambio de información sobre amenazas, vulnerabilidades y buenas prácticas. Más aún, necesita un continuo apoyo a la creación de CSIRTs sectoriales, y el financiamiento a la investigación y desarrollo de nuevas tecnologías.

La inversión en educación y concientización abarca las campañas de concientización pública, incorporar la ciberseguridad en la educación y fomentar la formación de profesionales especializados.

Considerando el impacto potencial y la viabilidad de las acciones de política pública en ciberseguridad, se propone la siguiente priorización:

Iniciativa	Impacto	Viabilidad
Fortalecer el marco regulatorio.	Alto. (proteger la infraestructura crítica y fomentar la inversión y mejora continua en base a los riesgos y amenazas globales)	Alta. (complementar la Ley Marco de Ciberseguridad 21.663 con Reglamentos Técnicos que accionen todas las atribuciones de la ANCI, e incorporar una regulación que permita la notificación pública de identificadores de compromiso que amenacen la seguridad nacional).
Fomentar la colaboración público-privada	Alto. (intercambio de información , respuesta a incidentes y estrategias)	Media. (crear mecanismos de confianza y voluntad de los sectores)
Campañas de concientización pública	Alto. (promover cultura de seguridad en el uso de tecnologías)	Alta. (campañas de bajo costo usando distintos medios de comunicación)
Incorporar ciberseguridad en la educación	Alto. (formar futuras generaciones y crear cultura de seguridad a largo plazo)	Media. (revisión de programas y formación docentes en ciberseguridad)
Financiar la investigación y desarrollo de nuevas tecnologías	Alto. (fomenta la innovación y la adaptación a las nuevas amenazas)	Media. (asignación de recursos y coordinación intersectorial)
Formación de profesionales especializados	Alto. (cubrir la demanda de talento)	Baja. (requiere crear programas especializados y la inversión en becas y ayudas)

→ 11.4 POTENCIALES INDICADORES DE ÉXITO

Para medir la efectividad de las acciones de política pública en ciberseguridad, se deben establecer indicadores de éxito claros y medibles. Estos indicadores permitirán evaluar el progreso y realizar ajustes en la estrategia si es necesario.

Iniciativa	Indicador
Fortalecimiento del marco regulatorio.	-Número de regulaciones en ciberseguridad implementadas. -Porcentaje de organizaciones que cumplen con las regulaciones. -Número de incidentes de ciberseguridad reportados. -Reducción en el impacto económico de los incidentes de ciberseguridad.
Fomento de la colaboración público-privada	-Número de plataformas de intercambio de información creadas. -Número de organizaciones que participan en las plataformas. -Frecuencia de intercambio de información entre el sector público y privado. -Número de CSIRTs sectoriales establecidos. -Eficiencia en la respuesta a incidentes de ciberseguridad.
Inversión en educación y concientización.	-Número de campañas de concientización pública lanzadas. -Alcance de las campañas (número de personas impactadas). -Nivel de conocimiento en ciberseguridad de la población. -Número de estudiantes que reciben educación en ciberseguridad. -Número de profesionales especializados en ciberseguridad formados.
Monitoreo y evaluación	-Los indicadores de éxito deben ser monitoreados periódicamente para evaluar el progreso del plan de acción. -Se deben realizar evaluaciones periódicas del impacto de las acciones de política pública en la ciberseguridad. -Los resultados de las evaluaciones deben ser utilizados para ajustar la estrategia y mejorar la efectividad de las acciones.

→ 11.5 LLAMADO A LA ACCIÓN PARA LA CIBERSEGURIDAD EN CHILE

La ciberseguridad es un desafío nacional que requiere la colaboración de todos los actores de la sociedad. Para construir un ciberespacio seguro y resiliente en Chile, hacemos un llamado a la acción a todos los sectores:

Gobierno	Sector privado	Academia	Sociedad civil
-Liderar el desarrollo e implementación de una estrategia nacional. -Priorizar la inversión estratégica en ciberseguridad. - Fortalecer la cooperación internacional en ciberseguridad.	-Implementar medidas de protección. -Invertir en la formación de sus empleados y adquirir tecnología segura. -Colaborar entre sectores.	-Promover I+D en ciberseguridad. -Formar nuevas generaciones. -Colaborar entre sectores.	-Tomar conciencia de la importancia de la ciberseguridad en la vida cotidiana. -Participar en iniciativas educativas. -Priorizar la ciberseguridad en organizaciones.

→ 12. CONCLUSIONES

En términos de Dominios del Modelo de Madurez de las Capacidades de Ciberseguridad para las Naciones de la Universidad de Oxford, debemos ponderar que en su universo, el Dominio 5 es el más extenso. Es por ello, la necesidad de su abordaje bajo subdominios o factores de interés. Para ser exactos, nos referimos a los hallazgos encontrados durante el proceso:

Cumplimiento de Estándares:

- Falta de un marco regulatorio nacional para ciberseguridad en TI y TO en la cadena de suministro.
- Diversidad de madurez en ciberseguridad entre sectores industriales y su cadena de suministro.
- Débil Gestión de Riesgos en la cadena de suministro.
- Barreras técnicas y económicas en la cadena de suministro.
- Dependencia de la cadena de suministro internacional.
- Servicios digitales de proveedores fuera o dentro del territorio nacional.

Controles de Seguridad:

- Fomentar una cultura de seguridad en toda la organización es fundamental para el éxito de cualquier programa de seguridad.
- Es necesario mantener un enfoque proactivo y estar al tanto de las últimas tendencias en ciberseguridad en base a la arquitectura y negocio.

• Los controles de seguridad deben adaptarse a las necesidades específicas de cada organización y el panorama de amenazas actuales.

• Seguir estándares y marcos de trabajo de controles globales, por ejemplo los integrados por NIST, COBIT, y CCM.

Calidad del Software

• El sector público tiene dificultades para integrar sistemas, carece de estandarización y tiene un presupuesto limitado para asegurar la calidad del software. El sector privado, por otro lado, se ve afectado por la presión de entregar software rápidamente y la falta de profesionales calificados en el área.

• Es necesario contar con metodologías ágiles y herramientas de gestión de proyectos, automatización de pruebas y análisis de código para asegurar la calidad del software.

• Para actualizar software de manera segura, se necesita realizar evaluaciones de riesgo. Además, es necesario un mantenimiento proactivo que utilice herramientas de monitoreo y estrategias de alta disponibilidad.

• Desafíos del sector público, aumentar la adherencia al estándar de desarrollo seguro de instituciones públicas.

• Desafíos del sector privado, homologar procesos de desarrollo con estándares DevSecOps y mejora en las herramientas de QA (acceso y utilización).

Comunicaciones e Internet Resiliencia de la Infraestructura

• Chile se enfrenta a la dificultad de proteger sus servicios esenciales debido a la constante evolución de las amenazas cibernéticas.

• Las organizaciones no son plenamente conscientes de los riesgos cibernéticos que enfrentan. Además, no todas las organizaciones comparten información sobre amenazas o no colaboran en la respuesta a incidentes.

• Chile debe adoptar estándares internacionales, y aplicar un enfoque de mejora continua que identifique, evalúe y proteja los activos de infraestructura crítica.

• La colaboración público-privada es clave para proteger la infraestructura crítica. Ambos sectores deben colaborar en el intercambio de información, desarrollo de estándares, financiación de la investigación y realización de simulacros.

• Para que la infraestructura de Internet de Chile sea resiliente, se necesita un enfoque integral que combine la adopción de estándares, la cooperación público-privada, la inversión en tecnologías y el desarrollo de capacidades a nivel nacional.

Mercado y Ciberseguridad

• El mercado de la ciberseguridad en Chile ha experimentado un crecimiento sostenible en los últimos años.

• El mercado chileno ha mostrado un crecimiento sostenido, aún se encuentra en una etapa de madurez temprana.

• El mercado chileno está conformado por una variedad de actores, incluyendo empresas multinacionales, empresas nacionales e startups.

• Sobre el 60% ponderó el factor "mi costo operativo se eleva" cuando se consultó, la reacción de la empresa a las nuevas regulaciones en materia de ciberseguridad en Chile.

• Al consultar sobre cuál indicador es el más relevante ante el mercado de la ciberseguridad, el 70% indicó que "el impacto de las regulaciones" es el tema de mayor interés.

Divulgación Responsable

• La limitada participación en el foro de ciberseguridad ha afectado significativamente la calidad del análisis y la toma de decisiones.

• Falta de iniciativas de colaboración a nivel privado y público para compartir información de vulnerabilidades y aprovechar sinergias.

• Aumento de la publicación de brechas y ciberataques con detalles sin control, ni seguir pauta bajo metodología TLP.

• Sobre exposición de casos de empresas atacadas en RRSS, con exposición de código y detalles, que pueden ser explotados por otros actores.

• Los controles de seguridad deben adaptarse a las necesidades específicas de cada organización y el panorama de amenazas actuales.

• Seguir estándares y marcos de trabajo de controles globales, por ejemplo los integrados por NIST, COBIT, y CCM.

Calidad del Software

• El sector público tiene dificultades para integrar sistemas, carece de estandarización y tiene un presupuesto limitado para asegurar la calidad del software. El sector privado, por otro lado, se ve afectado por la presión de entregar software rápidamente y la falta de profesionales calificados en el área.

• Es necesario contar con metodologías ágiles y herramientas de gestión de proyectos, automatización de pruebas y análisis de código para asegurar la calidad del software.

• Para actualizar software de manera segura, se necesita realizar evaluaciones de riesgo. Además, es necesario un mantenimiento proactivo que utilice herramientas de monitoreo y estrategias de alta disponibilidad.

• Desafíos del sector público, aumentar la adherencia al estándar de desarrollo seguro de instituciones públicas.

• Desafíos del sector privado, homologar procesos de desarrollo con estándares DevSecOps y mejora en las herramientas de QA (acceso y utilización).

Comunicaciones e Internet Resiliencia de la Infraestructura

• Chile se enfrenta a la dificultad de proteger sus servicios esenciales debido a la constante evolución de las amenazas cibernéticas.

• Las organizaciones no son plenamente conscientes de los riesgos cibernéticos que enfrentan. Además, no todas las organizaciones comparten información sobre amenazas o no colaboran en la respuesta a incidentes.

• Chile debe adoptar estándares internacionales, y aplicar un enfoque de mejora continua que identifique, evalúe y proteja los activos de infraestructura crítica.

• La colaboración público-privada es clave para proteger la infraestructura crítica. Ambos sectores deben colaborar en el intercambio de información, desarrollo de estándares, financiación de la investigación y realización de simulacros.

• Para que la infraestructura de Internet de Chile sea resiliente, se necesita un enfoque integral que combine la adopción de estándares, la cooperación público-privada, la inversión en tecnologías y el desarrollo de capacidades a nivel nacional.

→ Bibliografía

• Global Cyber Security Capacity Centre, GCSCC (2021). Cybersecurity Capacity Maturity Model for Nations (CMM). Department of Computer Science, University of Oxford. United Kingdom. Available on: https://gcscc.ox.ac.uk/

• Anderson, R. J., & Anderson, J. R. (2020). "Security Engineering: A Guide to Building Dependable Distributed Systems". Wiley.

• ISO/IEC 25010: Modelo de calidad para el software.

• ISO/IEC. (2018). ISO/IEC 27001:2018. International Organization for Standardization.

• Chen, X., & Paxson, V. (2021). "Operating System Security". University of California, Berkeley.

• Humble, J., & Farley, D. (2010). "Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation" . Addison-Wesley.

• Fitzgerald, B., & Stol, K. J. (2017). "Continuous Software Engineering: A Roadmap and Agenda" . Journal of Systems and Software.

• McClure, S., Scambray, J., & Kurtz, G. (2018). "Hacking Exposed: Network Security Secrets and Solutions". McGraw-Hill.

• Microsoft. (2020). Security Development Lifecycle (SDL). Microsoft.

• McGraw, G. (2020). "Software Security: Building Security In". Addison-Wesley.

• OWASP. (2023). OWASP Top Ten. OWASP Foundation.

• Ransome, J. F., & Misra, A. (2019). "Core Software Security: Security at the Source". CRC Press.

• Wills, A., & Hunt, D. (2021). "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws". Wiley.

• ITU-D (2015). Cybersecurity Program - Global Cybersecurity Index. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Cybersecurity-Index.aspx

• Estonian e-Governance Academy (2018). National Cyber Security Index. Retrieved from: https://ncsi.ega.ee/

• National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. https://www.nist.gov/cyberframework/framework

• Mordor Intelligence. Europa Ciberseguridad tamaño del mercado (s.f.). Disponible en: https://www.mordorintelligence.com/es/industry-reports/europe-cybersecurity-market.

• Mordor Intelligence Research & Advisory. (2023 , June). Análisis del tamaño y la participación del mercado de ciberseguridad en Chile, tendencias y pronósticos de crecimiento (2024 - 2029).

• Mordor Intelligence Research & Advisory. (2024 , February). Análisis del tamaño y la cuota del mercado europeo de ciberseguridad, tendencias y previsiones de crecimiento (2024 - 2029).

• Mordor Intelligence. Ciberseguridad en Chile Tamaño del Mercado. (s. f.). Disponible en: https://www.mordorintelligence.com/es/industry-reports/chile-cybersecurity-market.

• Santiago, J. M. El mercado en números. PrensarioHub. (2024). Disponible en: https://www.prensariohub.com/ciberseguridad-en-chile-el-mercado-en-numeros/

• Organización Internacional de Normalización. (2022). ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información [Norma]. Ginebra, Suiza: ISO.

• Center for Internet Security. (2021). CIS Controls v8. https://www.cisecurity.org/controls/v8

• Verizon. (2023). Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

• Comisión Europea. (2017). Marco Europeo de Interoperabilidad - una visión compartida y directrices para la administración pública europea en la era digital (COM(2017) 134 final). Bruselas.

• Waher, P. (2024). Open Threat Intelligence using Neuro-Ledger.

• Comisión Europea. (2023). Comunicación de la Comisión al Parlamento Europeo y al Consejo relativa al sexto informe de situación sobre la aplicación de la Estrategia de la UE para una Unión de la Seguridad [COM(2023) 665 final]. Bruselas

TRABAJO **FORO NACIONAL DE CIBERSEGURIDAD** 2024