CENTRO DE INNOVACION UC
ANACLETO ANGELINI

Microsoft

HOJA DE RUTA DE CIBERSEGURIDAD

14/17 Resumen ejecutivo

18/33 Contexto y diagnóstico

34/38 Metodología

39/47 Principales brechas en ciberseguridad

48/59 Trabajo de Comités de Desarrollo

60/65 Portafolio

66/68 Conclusiones y perspectivas futuras

69/74 Anexo

75/80 Referencias y bibliografía

MARÍA FRANCISCA YÁÑEZ
National Technology Officer Microsoft
Chair de la Hoja de Ruta

Hemos querido contribuir al desarrollo sustentable del país con esta Hoja de Ruta Digital. Los líderes que han trabajado en ella han generado un plan de acción muy concreto para los próximos tres años.

RAMÓN MOLINA
Director Ejecutivo
Centro de Innovación UC
Co-Chair de la Hoja de Ruta

Confiamos en que los lineamientos y proyectos propuestos en este documento, ejecutables en un plazo de tres años, contribuirán a que Chile pueda desarrollar una efectiva seguridad digital, convirtiéndose en un referente para la región.

CAROLINA TOHÁ
Ministra del Interior
y Seguridad Pública
Gobierno de Chile

El aporte de personas del mundo privado, público, gremios, academia y entidades internacionales, está robusteciendo nuestro debate, las decisiones que estamos tomando en esta materia. Este debate, junto a todos los esfuerzos que se están haciendo paralelamente, nos van a permitir estar más preparados como país ante esta temática relevante.

JUAN CARLOS MUÑOZ
Ministro de Transportes y Telecomunicaciones
Gobierno de Chile

Esta Hoja de Ruta de Ciberseguridad involucra transversalmente a toda la sociedad. Por lo mismo es claro que este documento va a servir como guía para el uso seguro de las tecnologías de la información y tecnologías de la comunicación, en una sociedad cada vez más integrada digitalmente.

SILVIA DÍAZ

Ministra de Ciencia, Tecnología, Conocimiento e Innovación
Gobierno de Chile

La ciberseguridad es una piedra angular de la era digital. Esta Hoja de Ruta permitirá consolidar un insumo valioso, que marcará directrices concretas en las cuales debemos trabajar como Ministerio de Ciencias.

COMITÉ ASESOR

Francisca Yáñez
Chair
National
Technology Officer
Microsoft

Ramón Molina
Co-Chair
Director Ejecutivo
Centro de
Innovación UC

Daniel Álvarez
Coordinador
Nacional de
Ciberseguridad
Ministerio del
Interior del
Gobierno de Chile

María Florencia
Attademo-Hirt
Gerente General
Países del Cono Sur y
Representante en Chile
Grupo BID

Carlos Aravena
Consultor Ciberseguridad,
Ciberdefensa y Seguridad
de la Información
Subsecretaría de Defensa
del Gobierno de Chile

Andrés Arce
Jefe de TI
Ministerio de
Ciencia, Tecnología,
Innovación y
Conocimiento del
Gobierno de Chile

Rodrigo Bon
Director Ejecutivo
ProPyme

Thierry de Saint
Pierre
Presidente
ACTI

Paula Estévez
Gerente General
AMCHAM

Marcelo Felman
Director
Ciberseguridad
Microsoft Latam

Álvaro García
VP Tecnología
Codelco

Eduardo Gorchs
CEO
Siemens

COMITÉ ASESOR

Martín Grosso
Corporate CIO
Cencosud

Fernando Hentzschel
Gerente de Capacidades Tecnológicas
Corfo

Ingrid Inda
Jefa de la División de Redes y Seguridad Informática
Ministerio del Interior y Seguridad Pública del Gobierno de Chile

Nicolás Majluf
Académico
Universidad Católica

Adolfo Oliva
Asesor de Gabinete Subsecretaría de Telecomunicaciones del Gobierno de Chile

Mario Ponce
Decano de la Facultad de Matemáticas
Universidad Católica

Kenneth Pugh
Senador de la República

Julián San Martín
Vicepresidente Mercado de Corporaciones
Entel

Patricio Subiabre
Gerente de Operaciones y Tecnologia
Banco BCI

Yerka Yukich
Presidenta
Alianza Chilena Ciberseguridad

COMITÉ DE DESARROLLO TALENTO EN CIBERSEGURIDAD

Álvaro Castro
INACAP

José Mguel Bejide
Instituto Profesional IACC

Wilson España
Sonda

Ricardo Fabelo
U. Gabriela Mistral

Joaquín Godoy
Chile Telcost

Marcelo Felman
Microsoft

Natalia López
Desarrollo país

Lina Marmolejo
Banco Interamericano de Desarrollo

Marco Perelli
Red de transformación digital

Romina Torres
U. Andrés Bello

Sebastián Vargas
Sociedad Chile de Seguridad de la Información

Ricardo Yáñez
DuocUC

Loreto Bravo
Universidad Del Desarrollo

Alejandro Jara
Universidad Católica

Ricardo León
País digital

Manuel Moreno
GlobalSecure

Claudio Ordónez
Accenture

Carolina Pizarro
NTT Data Chile

Marco Ponce
Sermaluc

COMITÉ DE DESARROLLO CULTURA EN CIBERSEGURIDAD

Jaime Astorquiza
Gobierno Digital

Felipe Castro
(ISC)² Chile Chapter

Rosario Castro
Banco Security

Mauricio Fierro
CMPC

Macarena Gatica
Alessandri Abogados

Pamela Gidi
Consultora

Joaquín Godoy
Chile Telcost

Facundo Jamardo
EY

Luis Malca
Sermaluc

Claudio Ordóñez
Accenture

Paula Ortega
Entel

Claudia Santa Ana
Microsoft Chile

Ximena Tapia
Microsoft

Francisco Valenzuela
CETIUC

Karina Vidal
Red Chilena de Transformación Digital A.G.

Marcelo Wong
Policía De Investigaciones

Jaime Lama
Instituto de Neuroliderazgo

Ricardo León
Fundación País Digital

Marco Ponce
Sermaluc

Puppy Rojas
Chile Telcos

Fernando Sánchez
Fundación País Digital

Alfie Ulloá
Chile Telcos

Cristián Vega
ABIF

COMITÉ DE DESARROLLO TECNOLOGÍA, ECOSISTEMA, PROTOCOLOS Y ESTÁNDARES

Jocelyn Arteaga
Bupa

Soledad Bastías
Codelco

Carlos Bustos
SONDA

Marcelo Dalceggio
Cencosud

Benjamín Díaz
Microsoft

Robinson Cáceres
Security

Alberto Castañeda
NETprovider

Felipe Castro
(ISC)² Chile Chapter

Miguel Cisterna
Telefónica

Mauricio Fierro
CMPC

Rodrigo Tapia
Sermaluc

Hugo Galilea
Kepler

Sebastián Izquierdo
Izquierdo & Hurtado Abogados

Enrique Letelier
Ejército de Chile

Diego Macor
IBM

Paola Molina
Microsoft Chile

Paula Ortega
Entel

Rodrigo Reveco
Red de transformación digital

Alfredo Rolando
Siemens

Romina Torres
U. Andrés Bello

Katherina Canales
Global Cyber

Eduardo Correa
CEN

Juan Downey
ABIF

Michael Heavy
INCIBER

Jorge Labayru
Microsoft

Patricio Leyton
CEN

Marcelo Maraboli
Universidad Católica

Carlos Monroy
Clínica Alemana

Juan Luis Núñez,
TMG

Claudio Pino
SIGPA

Marco Ponce
Sermaluc

Renato Vanzulli
ESVAL

Javier Zorzo
Telefónica

EQUIPO EJECUTIVO

CENTRO DE INNOVACIÓN UC ANACLETO ANGELINI

Marcela Briones
Subdirectora Comunicaciones y Asuntos Corporativos

Francisco Pizarro
Subdirector de I+D con la Industria

Rocío Ortiz
Jefe de Industrias del Futuro

Pamela Silva
Coordinadora de Branding y Eventos

Philippe Werner-Wildner
Coordinador de Asuntos Corporativos

MICROSOFT CHILE

Pía Baeza
Integrated Marketing Coordinator

Tamara Vildósola
Gerente de Marketing Microsoft Chile

Natalia Torres
Directora de Comunicaciones

0.1 RESUMEN EJECUTIVO

RESUMEN EJECUTIVO

La disponibilidad de la tecnología y de la información ha permitido que en los últimos años, el proceso de adopción de **la transformación digital en las organizaciones privadas, el sector público y en la sociedad civil se haya acelerado con grandes beneficios para las personas y las organizaciones. Esta aceleración creció de forma exponencial, especialmente a propósito de la última crisis sanitaria provocada por el Covid-19 desde el año 2020.**

Dentro de este contexto, y a propósito de la necesidad de recuperación económica del país, es que en el marco del Plan Transforma Chile, anunciado por Microsoft Chile en diciembre de 2020, durante 2021 se desarrolló la **Hoja de Ruta de Transformación Digital para la Reactivación Económica,** co-liderada por Microsoft Chile y el Centro de Innovación UC Anacleto Angelini. Dentro de las reflexiones realizadas por este grupo de trabajo, se concluyó que la adopción tecnológica asociada a la transformación digital de la cadena productiva nacional abría un espacio de vulnerabilidad y de exposición importante a ciberataques si no se realizaba tomando las medidas de seguridad correspondientes. Por lo tanto, **esta transformación no podía hacerse realidad sin una estrategia de ciberseguridad que permitiera la protección de los negocios, de la infraestructura crítica y de los datos personales de los usuarios y consumidores.** De ahí que la propuesta de este equipo de trabajo estableció la necesidad de desarrollar una **Hoja de Ruta especializada en ciberseguridad.**

Se sabe con certeza que este escenario amplía el espacio de exposición a riesgos que tienen las personas y las organizaciones, abriendo un flanco digital importante para las brechas de seguridad. Un ejemplo de cómo escalan las amenazas digitales y la ciberactividad delictual, se refleja en que en la **actualidad, son analizadas diariamente 43 trillones de señales potencialmente riesgosas a nivel global** (Microsoft, 2022), mientras en 2021 ese número llegaba a 29 trillones.

Este fenómeno se vivió de manera particularmente intensa en Chile durante los últimos años, con los ciberataques que son de público conocimiento.

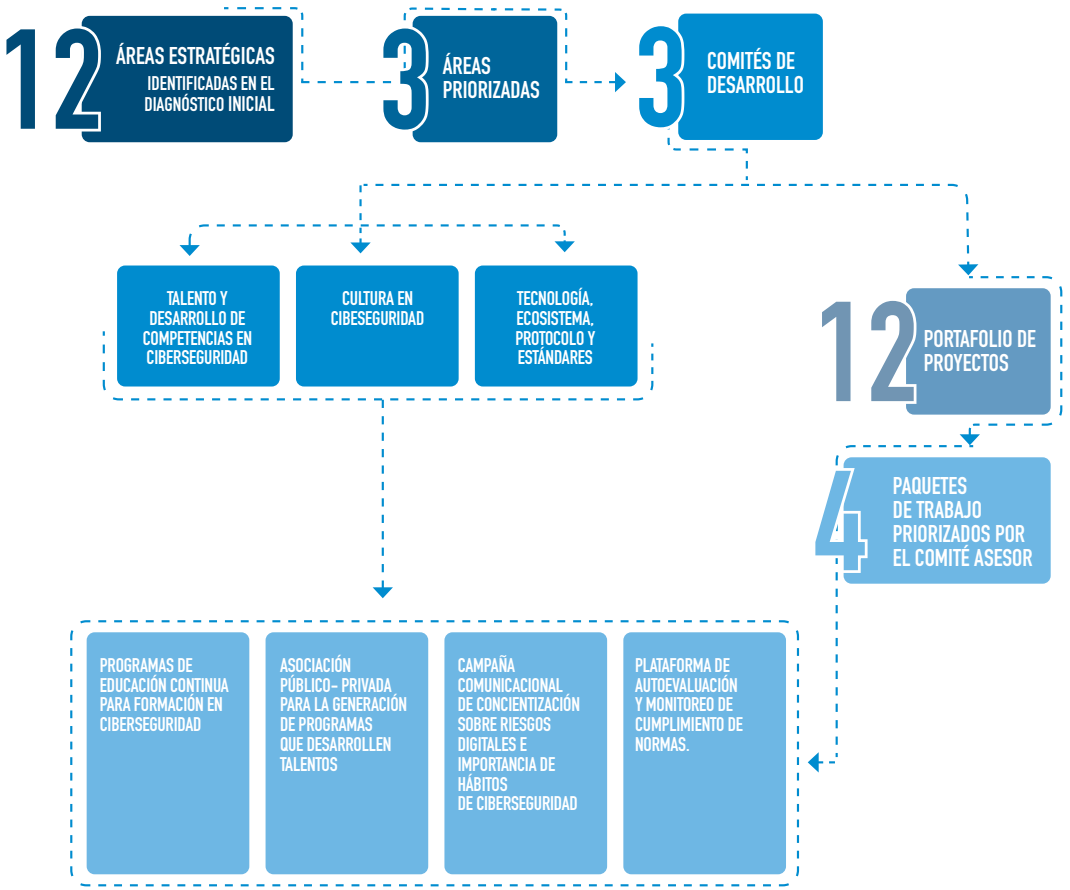
Estas acciones evidencian que el valor de construir la Hoja de Ruta de Ciberseguridad reside en su proceso, ya que permite unificar problemáticas comunes en torno a un diálogo intersectorial, para conducir a la elaboración de paquetes de trabajo que puedan ejecutarse a nivel país hacia 2025.

En el desarrollo de esta Hoja de Ruta **participaron activamente alrededor de cien profesionales líderes en su área a nivel nacional,** durante ocho meses, en dos instancias:

- El **Comité Asesor**, integrado por directores, directoras y gerentes de grandes empresas del país, además de líderes del sector público, organismos internacionales, referentes de las pymes y la academia. Su objetivo fue establecer las bases de una visión preliminar de la problemática, instaurando una mirada estratégica y una priorización de las áreas y brechas que se profundizan en cada uno de los Comités de Desarrollo.
- Los **Comités de Desarrollo**, integrados por representantes de diversas organizaciones, que cuentan con experiencias en iniciativas privadas, públicas y académicas asociadas a las áreas detectadas. Se formó un Comité por cada área priorizada (Cultura, Talento y Tecnología) con el objetivo de instaurar una mirada táctica y operativa por medio de la propuesta de proyectos concretos a implementar.

Inicialmente, el equipo ejecutivo de la Hoja de Ruta trabajó junto al Comité Asesor en la construcción de un diagnóstico sobre el estado de la ciberseguridad en Chile, lo que derivó en la definición de doce áreas. Este trabajo consistió en levantar la visión común de los distintos participantes del Comité Asesor a través de una revisión del estado del arte y la realización de más de veinte entrevistas semi-estructuradas a los miembros del Comité y otros profesionales relevantes por su conocimiento técnico del área.

Desde una mirada estratégica, **el Comité Asesor priorizó tres de las doce áreas de intervención**, que dieron origen a los Comités de Desarrollo (“Talento y Desarrollo de Competencias en ciberseguridad”; “Cultura en ciberseguridad”; Tecnología, ecosistemas, protocolos y estándares”). Con la formación de ellos, se convocó a actores relevantes en la materia, en línea con el espíritu colaborativo y la mirada país del proyecto. Una vez concluidas las sesiones de trabajo de los Comités de Desarrollo, el Comité Asesor adoptó un rol de análisis y priorización de los proyectos propuestos. Todo este proceso metodológico se explica gráficamente en el siguiente diagrama.



Esta Hoja de Ruta 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. De esta manera, se diferencia de otros documentos en que no se queda sólo en e ejercicio teórico, sino que propone **proyectos concretos, ejecutables en un horizonte de tres años.** De hecho, al momento de presentar este documento, varios de los proyectos ya están siendo ejecutados.

Una de estas iniciativas que ya está en ejecución es el primer piloto Mínimo Producto Viable de una **academia de seguridad, impulsado por la Universidad Católica y Microsoft.** De manera ágil y transversal fueron convocados los estudiantes de todas las facultades de la universidad, de los cuales 450 están en proceso de certificación, tras participar en un programa de formación digital y aprobar un examen. Esta iniciativa ha permitido formar a profesionales nativos en ciberseguridad, en carreras tan diversas como ingeniería, ciencias sociales y áreas de la salud.

La invitación, por lo tanto, es a encontrar los espacios de sinergia y de co-construcción que permitan avanzar en el nivel de madurez de ciberseguridad necesario para el desarrollo del país y para el posicionamiento como referentes regionales.

0.2 CONTEXTO Y DIAGNÓSTICO

CONTEXTO Y DIAGNÓSTICO

ANTECEDENTES

Producto de la crisis económica derivada del cierre de los comercios y las cuarentenas necesarias para combatir los efectos del Covid-19, sumado a las presiones de los mercados internacionales, las interrupciones de las cadenas de suministro, el aumento en el precio de los principales commodities y el aumento sostenido de los precios en el mercado nacional, se detonó una presión importante en el sector productivo y, en especial, en los segmentos más vulnerables del país, como las MIPYMES. Es aquí donde surge la oportunidad de apalancar tecnologías y recursos digitales para habilitar la recuperación de la economía y desarrollar nuevos modelos de negocios. **La disponibilidad tecnológica y de información ha permitido que en los últimos años, y especialmente a propósito de la última crisis sanitaria de 2019, el proceso de adopción de la transformación digital en las organizaciones privadas, el sector público y en la sociedad civil se haya acelerado de forma exponencial.**

Dentro de este contexto, y a propósito de la necesidad de recuperación económica, es que en 2021 se desarrolló una **Hoja de Ruta de Transformación Digital para la Reactivación Económica,** co-liderada por Microsoft Chile y el Centro de Innovación UC Anacleto Angelini, que logró convocar a más de **sesenta organizaciones del sector público, privado, académico y civil** que participaron en un proceso de co-construcción de un diagnóstico compartido y el desarrollo conjunto de un portafolio de iniciativas colaborativas para apoyar la reactivación económica por medio de la transformación digital. **El objetivo de esta iniciativa fue desarrollar proyectos concretos a tres años plazo, que permitieran facilitar la incorporación de herramientas digitales con foco en los segmentos de las pequeñas y medianas empresas, jóvenes y ciudadanía.** Esta iniciativa derivó en la publicación de un **portafolio de siete paquetes de trabajo** enfocados en las áreas de talento digital, brechas digitales, adopción tecnológica y cultura digital en las organizaciones.

Dentro de las reflexiones derivadas de este grupo de trabajo se definió que la adopción tecnológica asociada a la transformación digital de la cadena productiva del país abría un espacio de vulnerabilidad y de exposición importante si no se realizaba tomando las medidas de seguridad correspondientes. Por lo tanto, **esta transformación no podía hacerse realidad sin una estrategia de ciberseguridad que permitiera la protección de los negocios, de la infraestructura crítica y de los datos personales de los usuarios y consumidores.** De ahí que la propuesta del equipo de trabajo de la Hoja de Ruta de Transformación Digital para la Reactivación Económica 2021 estableció la necesidad de desarrollar una Hoja de Ruta especializada en temas de ciberseguridad, que permitiera abordar esta área en todas sus dimensiones y desarrollar un portafolio de proyectos adecuados para facilitar la transformación digital del país por medio de mecanismos de protección resilientes y colaborativos.

ACOMPAÑAR EL PROCESO DE MADUREZ TECNOLÓGICA Y DIGITAL A UNA ESCALA LOCAL Y REGIONAL

La Hoja de Ruta de Ciberseguridad 2022 busca desarrollar una bajada táctica y colaborativa entre el sector público, privado, civil y la academia para abordar las brechas de ciberseguridad a nivel país. Además, podrá acompañar el proceso de madurez tecnológica y digital a una escala local y regional. Para este propósito, este año se ha convocado a importantes representantes de múltiples organizaciones y sectores del ecosistema a definir los lineamientos estratégicos prioritarios de esta Hoja de Ruta por medio de un Comité Asesor y la definición de las primeras iniciativas de trabajo durante los primeros tres años, mediante Comités de Desarrollo.

CIBERSEGURIDAD Y CONTINGENCIA, ALGUNAS CIFRAS

Una parte central de la promesa de valor de la llegada de la Industria 4.0 es la dilución de la barrera física y cibernética, lo que ha empujado hacia la integración de los sistemas de información y de operaciones, de la cual deriva la generación de datos de operación y de usuario de altísimo volumen y complejidad. Esta dimensión de la transformación digital habilita una serie de oportunidades para el desarrollo económico y de país. **En 2017, Mckinsey ya estimaba el impacto de la transformación digital en empresas reinventadas digitalmente, proyectando un aumento de ventas, ganancias antes de intereses e impuestos y retorno sobre la inversión de entre el 2X y 2,5X** (Mckinsey, 2017). Esta oportunidad de crecimiento se expande aún más si consideramos que para 2022 se estimaba que la cantidad de dispositivos conectados sería de 46 miles de millones a nivel mundial, esperando al 2030 un salto a más de 125 miles de millones (Statista, 2022). Tan sólo en Chile existen más de 25 millones de dispositivos móviles conectados (DataReportal, 2021).

Sin embargo, este escenario amplía el espacio de exposición a riesgos que tienen las personas y las organizaciones, abriendo un flanco digital importante para las brechas de seguridad. Por ejemplo, **de acuerdo al reporte de Cybersignals 2021, en un mes ocurrieron más de 83 millones de ataques cibernéticos a nivel mundial** (Microsoft, 2021). Este fenómeno se ha agudizado aún más considerando que las empresas aumentaron la intensidad del trabajo remoto, exponiéndose a filtraciones de datos más costosas. Los ciberataques cuestan más de 1 millón de dólares en promedio, y al comparar el trabajo presencial con el remoto, este último eleva el costo en un 27% (IBM Corporation, 2021).
Adicionalmente, **se estima que a las empresas de todo el mundo les costará 6 billones de dólares reparar los efectos de los ciberataques en 2021, un aumento del 100% desde 2015** (Morgan, 2020).

Ni siquiera las grandes empresas están libres de estos riesgos. El 31 de marzo de 2022, Apple y Meta sufrieron una filtración de datos a partir de un ciberataque que involucró suplantación de identidad y phishing (Aguiar, 2022). Esta tendencia ha permeado los directorios y la preocupación a nivel estratégico de los altos ejecutivos, lo cual se puede ver con claridad en la PwC 25th Annual Global CEO Survey, en la cual los CEO consultados ranquean los ciber-riesgos como la principal amenaza de crecimiento, dentro de los próximos doce meses (PwC, 2022).

Así mismo, si consideramos segmentos más vulnerables, como las pequeñas y medianas empresas, el problema se agudiza aún más. El estudio Impacto de COVID-19 en la cultura y operación de las Pymes chilenas, de Microsoft Chile, señala que **nueve de cada diez empresas declararon que la pandemia aceleró la transformación digital de su negocio** por medio de la adopción tecnológica, y el 93% de ellas menciona haber realizado alguna inversión para facilitar el teletrabajo. Por ejemplo, y el 85% dijo haber utilizado datos y analítica para la toma de decisiones (Microsoft Latinoamérica, 2022). Gran parte de este avance hacia la digitalización en el sector PYME ha sido estimulado por políticas de Gobierno como los Programas de Digitalización "Digitaliza tu PYME", del Ministerio de Economía, que en octubre de 2021 ya reportaba más de 400.000 PYMES digitalizadas por medio de sus programas (Minecon, 2021). Este segmento de empresas, sin embargo, se ha visto atacado por amenazas cibernéticas con cada vez más frecuencia. **De acuerdo a Forbes, las pequeñas empresas son tres veces más susceptibles a ataques por cibercriminales que empresas de mayor tamaño** (Forbes, 2022).

La transformación digital en las organizaciones, y su acelerada adopción, ha propiciado las condiciones para poner el foco de manera urgente y necesaria en la ciberseguridad. La hiperconectividad digital, la economía digital y la Industria 4.0 han detonado grandes beneficios, que han permitido, por ejemplo, que hoy en día se genere por minuto una cantidad de datos impresionante. Tan sólo en sesenta segundos se gastan más de 1,6 millones de dólares online, se suben más de 500 horas de contenido a Youtube y se envían más de 198 millones de correos.

Este contexto abre espacios importantes de oportunidad, considerando que hoy en día se estima que existen más de 46 mil millones de dispositivos conectados a nivel mundial, esperando al 2030 un salto a más de 125 mil millones.

CANTIDAD ESTIMADA DE DATOS CREADOS EN INTERNET EN 1 MINUTO

De este contexto se deduce la importancia estratégica de la ciberseguridad para Chile y la región, así como de la oportunidad de desarrollar ventajas comparativas importantes en el ecosistema, que permitan un desarrollo económico y social seguro y sostenible para la ciudadanía. **Con el fin de elaborar una propuesta de valor se propone como marco de trabajo la metodología de Hoja de Ruta, la cual se basa en un proceso de co-construcción privado, público, académico y con participación civil, que permite unificar problemáticas tan complejas como la ciberseguridad,** en torno a brechas y oportunidades comunes del ecosistema.

FUENTE: GLOBAL CYBERSECURITY OUTLOOK 2022

DEFINICIONES BASALES SOBRE CIBERSEGURIDAD

Un punto de partida fundamental es entender el alcance de la definición que se use de ciberseguridad y comprender por qué tiene una relevancia estratégica para el trabajo de esta Hoja de Ruta.
Dependiendo del proveedor tecnológico o de la referencia bibliográfica se pueden encontrar distintas aproximaciones y definiciones técnicas del término ciberseguridad. Por ejemplo, IBM define la ciberseguridad como: "Práctica de proteger los sistemas críticos y la información confidencial de los ataques digitales. También conocidas como seguridad de la tecnología de la información (TI), las medidas de seguridad cibernética están diseñadas para combatir las amenazas contra los sistemas y aplicaciones en red, ya sea que esas amenazas se originen desde dentro o fuera de una organización". (IBM Corporation, 2022).

Otra definición es la que CISCO realiza y en la que presenta la ciberseguridad como "la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ciberataques suelen tener como objetivo acceder, modificar o destruir información confidencial; extorsionar a los usuarios; o interrumpir los procesos comerciales normales" (CISCO, 2022).

El problema es que en este marco de definiciones se puede caer en considerar la ciberseguridad como algo netamente técnico que hay que derivar a las áreas de TI o los CISO únicamente. Sin embargo, **la invitación de esta instancia de Hoja de Ruta es a empujar la ciberseguridad como una temática más allá de una dimensión técnica.**

Este punto se sostiene sobre la base de que los esfuerzos asociativos del ecosistema están centrados en la reactivación y crecimiento económico, y en el bienestar del país. Estos objetivos se gestionan y operacionalizan por medio de decisiones de negocios y de política pública que se habilitan por medio de la información como activo estratégico y fundamental. De aquí nace la relevancia de la definición de ciberseguridad en un sentido amplio, más allá de la tecnología misma.

Si consideramos un alcance mucho más completo y amplio, dentro del ámbito de la seguridad de la información, se logra llegar a un concepto en donde la ciberseguridad se puede entender como:

> Un **proceso integral sistemático** que permite mantener la **confidencialidad, integridad y disponibilidad** de la información en todas sus etapas, así como su infraestructura asociada, por supuesto, por medio de la implementación de políticas y protocolos, programas de entrenamiento, campañas de concientización y la adopción e integración de tecnología.
>
> (Adaptación libre de Management of Information Security 6th Edition, 2018)

Bajo esta definición, se abre un espacio de intervención mayor en donde ya no se trata sólo de software y hardware, sino de otras dimensiones complementarias igualmente relevantes en donde el rol de cada actor del ecosistema es fundamental para catalizar un proceso de aceleración y visualización de la importancia de la ciberseguridad de forma transversal. De esta manera, elementos como la cultura digital, los nuevos modelos de negocio, el talento en ciberseguridad, los protocolos y buenas prácticas, la regulación, la gobernanza, la infraestructura habilitante y el desarrollo tecnológico, entre otros, toman especial protagonismo dentro de la discusión.

Dentro de esta sección de definiciones es igualmente relevante considerar la distinción entre dos conceptos relevantes: ciberseguridad y ciberdefensa.

La ciberdefensa implica capacidades ofensivas, defensivas y de inteligencia, enfocadas en la protección nacional, la soberanía y protección de las instituciones militares. Si bien existen elementos comunes, en esta Hoja de Ruta se hará referencia exclusivamente a la definición de ciberseguridad, dejando fuera los ámbitos de ciberdefensa de la discusión. Por supuesto, existen espacios de intersección relevantes en donde se pueden generar sinergias para plantear la ciberseguridad y sus aprendizajes dentro de la esfera pública y de país.

TIPOS DE AMENAZAS EN CIBERSEGURIDAD

Existen distintas clasificaciones de las amenazas de ciberseguridad. CISCO (2022), por ejemplo, describe cuatro grandes categorías importantes:

Phishing: Es el tipo más común de ciberataque y consiste en el envío de correos electrónicos fraudulentos, que aparentan ser emails legítimos de fuentes confiables, con el objetivo de robar datos sensibles.

Ransomware: Es un tipo de software malicioso diseñado para extorsionar a las organizaciones por medio del bloqueo del acceso a sus sistemas, el cual se libera sólo cuando se paga un rescate definido por los secuestradores.

Malware: Es otro tipo de software que tiene como objetivo obtener acceso no autorizado a los sistemas. Puede estar diseñado para extraer información o para causar daños o fallas en los sistemas infectados.

Ingeniería social: Es un término referido a tácticas que requieren interacción humana para obtener, mediante engaños o manipulación, el acceso a información confidencial.

Estas cuatro categorías componen el grupo más importante de ataques y brechas de seguridad a nivel mundial. Así mismo, existe otro tipo de ataques que pueden considerarse como parte de las amenazas a la ciberseguridad, en el sentido más amplio de la definición. En el libro *Management of Information Security 6th Edition* (2018) se plantean doce categorías de amenazas a la ciberseguridad, definidas como cualquier evento o circunstancia que puede suponer peligros para la organización, sus personas, información y sistemas. Se consideran ámbitos asociados a:

1. Compromisos a la propiedad intelectual
2. Desviaciones en la calidad de servicio, como las intervenciones asociadas a energía, por ejemplo, *blackouts, browns-outs* u otros que afecten el *up-time* de los servicios y que pueden afectar gravemente al sector industrial
3. Espionaje o acceso no autorizado, ya sea a nivel industrial o de violación de credenciales de acceso y contraseñas, lo cual puede hacerse por medio de mecanismos de ataques tecnológicos o por medio de ingeniería social
4. Fuerzas de la naturaleza que puedan dañar equipos o redes de infraestructura
5. Error humano o fallos en el cumplimiento de protocolos de seguridad
6. Extorsión de información
7. Sabotaje o vandalismo
8. Ataque de software, donde se pueden clasificar los *ransomware* y *malware* previamente mencionados. En esta categoría están los virus, los troyanos y el *spam*, entre otros
9. Fallos técnicos de *hardware*
10. Sabotaje o vandalismo
11. Obsolescencia técnica
12. Robos de activos físicos

Cualquiera de estas amenazas puede afectar alguno de los elementos de la llamada triada de la ciberseguridad, ya sea impactando la utilidad o usabilidad de los activos de la organización; la posesión de estos activos; o la privacidad de ellas, por medio de la afectación de alguno de sus elementos de integridad, disponibilidad o confidencialidad previamente descritos. Todo lo anterior coarta la existencia de información para la toma de decisiones rápida y confiable en cualquier proceso de negocios de una organización (*Management of Information Security 6th Edition, 2018*).

INCIDENTES DE CIBERSEGURIDAD

En los últimos años, se han desarrollado una serie de incidentes de ciberseguridad mediáticos que han catalizado el aumento de la atención relativa al tema. **De acuerdo a un reporte de Deloitte, el 64% de las empresas de todo el mundo ha sufrido al menos una forma de ciberataque. Existen cerca de 90 millones de ciberataques por día y el correo electrónico se posiciona como el responsable de alrededor del 91% de todos los ciberataques** (2020).

En esta misma línea, de acuerdo a reportes del 2021, el uso de ataques vía ***malware*** aumentó un 358% hasta 2020 y el uso de ransomware aumentó un 435% en comparación con 2019 (Deep Instinct, 2020). A nivel latinoamericano, se observa que el año 2022 México fue el país dentro de Latinoamérica que más intentos de ataques recibió seguido de Brasil, Perú y Colombia, con 156 mil millones, 88,5 mil millones, 11,5 mil millones y 11,2 mil millones respectivamente (FortiGuard Labs, 2022 en DF 2022). En esta línea, el mismo estudio menciona que **"Chile sufrió más de 9,4 mil millones de intentos de ciberataques en 2021, cerca de cuatro veces más que los detectados en 2020"** (Diario Financiero, 2022). Estas cifras dan cuenta del nivel de exposición y crecimiento de los ataques de ciberseguridad a nivel regional y la relevancia de establecer mecanismos para prevenir y mitigar su impacto.

SECTORES AFECTADOS POR INCIDENTES DE CIBERSEGURIDAD

Los tipos de empresas u organizaciones que son más vulnerables a los ciberataques incluyen bancos e instituciones financieras, instituciones de atención médica, corporaciones e incluso educación superior (Embroker, 2019). Esto deja en exposición los datos personales de clientes, pacientes, empleados e incluso productos y procesos industriales sujetos a propiedad intelectual.

En Chile, en particular, han existido ataques como el de Banco de Chile, que causó pérdidas por sobre los 10 millones de dólares, en 2018 (Radio Bio Bio, 2018). Así mismo el 2020 Bancoestado sufrió un ciberataque, que obligó a la empresa a cerrar sus sucursales (El Mostrador, 2020).

En septiembre de 2022, el Subsecretario del Interior, Manuel Monsalve, confirmó que el Estado Mayor Conjunto fue objeto de un ciberataque en mayo de ese año. El grupo hacktivista Guacamaya liberó más de 300 mil archivos del órgano, entre los que se encuentran apreciaciones sobre el estallido social, y gastos de las Fuerzas Armadas durante el Estado de Excepción en las regiones del Biobío y La Araucanía, bajo el Gobierno de Sebastián Piñera, entre otros (El Mostrador, 2022). A los pocos días, el Departamento de Informática del Poder Judicial fue víctima de un ciberataque de carácter Cryptolocker

(Ransomware), reportando que un virus infectó al 1% de sus computadores, lo que terminó por afectar a los equipos y no a los sistemas informáticos. Este tipo de ataques, por supuesto, generan problemas no sólo a nivel operativo y de negocios, sino que también erosionan la confianza en las instituciones y friccionan la interacción de la ciudadanía con los servicios digitales privados y públicos (Emol, 2022).

TIEMPO DE REACCIÓN ANTE ATAQUES DE CIBERSEGURIDAD

Una dimensión fundamental asociada a los ciberataques es el tiempo de reconocimiento y de acción que tienen actualmente las empresas. El estudio Cyber Signals 2021 de Microsoft señala que los atacantes tardan 12 minutos en accedes a los datos privados y 30 en acceder a casi toda la información privada. Además, se estima que una organización Se estima que una organización tarda 197 días en descubrir el ciberataque y hasta 69 en contenerlo (IBM, 2020). En esta línea, los tiempos de respuesta a este tipo de ataques son críticos y reportan un impacto directo, en donde, compañías que logran contener un ataque en menos de 30 días pueden ahorrar hasta más de 1 millón de dólares en comparación con el grupo que tarda más de 30 días en contener el incidente (IBM, 2020). Respecto a este punto, se vuelve crucial contar con capacidades no sólo de prevención, sino también de detección temprana, contención inmediata y control de daños provocados por las brechas de ciberseguridad que afectan a las organizaciones.

COSTOS DE LA BRECHAS DE CIBERSEGURIDAD

Cifras del Informe de Defensa Digital de Microsoft 2021, señalan que la ciberdelincuencia aumentó en un 600%. Este número sigue creciendo, al igual que la inversión en ciberseguridad; a 2021, éste alcanzaba seis trillones de dólares en todo el mundo, el doble de lo que se gastaba en 2015.

Los costos de las brechas de ciberseguridad no sólo se ven reflejados en los impactos financieros mencionados anteriormente, y que se derivan del impacto en la interrupción operativa o el valor de los ingresos no percibidos. Existen otras dimensiones importantes a considerar y que revelan la importancia estratégica transversal en las distintas áreas de la organización. Deloitte, en su estudio de 2016 detalla de forma importante los llamados **“costos ocultos” de los ciberataques,** que incluyen consideraciones tales como el aumento en las **primas de seguro** en los que se deben incurrir tras enfrentar un incidente, así como el aumento en el **costo de la deuda** derivado de este mismo fenómeno. Dimensiones como la **pérdida o compromiso de la propiedad intelectual, además de la devaluación del nombre comercial y daño en la confianza de los clientes”**, son otros aspectos que se ven afectados (Deloitte, 2016). Este análisis es relevante para dimensionar que la ciberseguridad no sólo impacta a nivel operacional o técnico, sino que también involucra de forma transversal a diversas áreas claves de la compañía. Esto demuestra la importancia de una aproximación integral hacia la problemática.

NIVELES DE MADUREZ EN CIBERSEGURIDAD: MEDICIONES Y RANKINGS

Entendiendo el impacto que pueden tener los ataques de ciberseguridad en las organizaciones, es sumamente relevante entender cómo han avanzado los países en términos de esfuerzos para implementar mejores políticas de ciberseguridad y facilitar el desarrollo de ecosistemas nacionales robustos. **Existen dos importantes mediciones asociadas al nivel de madurez en ciberseguridad nacional: el Global Cybersecurity Index desarrollado por el ITU y el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM),** desarrollado por Oxford con apoyo de la OEA y el BID para su implementación en América Latina.

El Global Cybersecurity Index considera cinco grandes dimensiones de análisis: (1) Medidas Legales, (2) Medidas Técnicas, (3) Medidas Organizacionales, (4) Desarrollo de Capacidades, y (5) Cooperación (ITU, s/f). El objetivo de este índice es generar conciencia de las brechas existentes en los distintos ecosistemas y establecer una referencia sobre el nivel de compromiso de los países respecto a la implementación de medidas para el desarrollo de la ciberseguridad. **En este ranking, Chile se posicionó el 2020 en el puesto 74, con sus fortalezas en la dimensión legal y sus principales debilidades en la implementación de medidas técnicas** (ITU, 2020).

Por otro lado, el **Modelo de Madurez para las Naciones de Oxford (2020)** contempla cinco grandes dimensiones de medición e intervención:

1. POLÍTICA Y ESTRATEGIA DE CIBERSEGURIDAD: DISEÑO DE ESTRATEGIA Y RESILIENCIA DE CIBERSEGURIDAD
2. CULTURA CIBERNÉTICA Y SOCIEDAD: FOMENTAR UNA CULTURA DE CIBERSEGURIDAD RESPONSABLE EN LA SOCIEDAD.
3. EDUCACIÓN, CAPACITACIÓN Y HABILIDADES EN CIBERSEGURIDAD: DESARROLLO DEL CONOCIMIENTO DE CIBERSEGURIDAD.
4. MARCOS LEGALES Y REGULATORIOS: CREACIÓN DE MARCOS LEGALES Y REGULATORIOS EFECTIVOS.
5. ESTÁNDARES, ORGANIZACIONES Y TECNOLOGÍAS: CONTROL DE RIESGOS A TRAVÉS DE ESTÁNDARES, ORGANIZACIONES Y TECNOLOGÍAS.

En este índice, Chile se posiciona en niveles entre dos y tres, de un máximo alcanzable de cinco niveles de madurez posibles, que van desde la inicial hacia la formativa, luego consolidada y la más avanzada (dinámica). Las dimensiones más desarrolladas, que se encuentran en niveles cuatro a cinco son aquellas asociadas al desarrollo de una estrategia nacional, leyes de propiedad intelectual, protección al consumidor, entre otras de carácter estratégico y regulatorio. Las brechas del índice de Oxford, consistentes con el diagnóstico de ITU, aparecen en las dimensiones asociadas a la implementación tecnológica y táctica, así como en el desarrollo de marcos de formación (OEA, 2020).

Estas mediciones son fundamentales para entender la línea base de trabajo sobre la cual se debe continuar para construir e implementar iniciativas que empujen hacia avanzar a mayores niveles de madurez de forma progresiva sostenible.

IMPORTANCIA REGIONAL DE LA CIBERSEGURIDAD

Las brechas previamente descritas han empujado hacia el desarrollo de compromisos por parte de las naciones y los distintos organismos a los que estas pertenecen, lo cual da cuenta de la importancia de la ciberseguridad en las estrategias nacionales, regionales e internacionales. Por ejemplo, en la **Cumbre de las Américas de junio 2022, se firmó la Agenda Regional para la Transformación Digital** (IX Summit of the Americas), acuerdo que también suscribió Chile y el cual estableció siete grandes puntos, cuyos títulos generales se presentan a continuación:

1. ACCIONES DE COOPERACIÓN CON ORGANISMOS INTERNACIONALES, ENTIDADES PÚBLICAS REGIONALES Y EQUIPOS DE RESPUESTA A EMERGENCIAS INFORMÁTICAS (CERTS)
2. IMPULSO AL DESARROLLO DE TALENTO DIGITAL ESPECIALIZADO EN CIBERSEGURIDAD EN LA REGIÓN
3. FOMENTO DE LA DISCUSIÓN DE ESTÁNDARES Y EL INTERCAMBIO DE MEJORES PRÁCTICAS EN LAS ÁREAS DE CIBERSEGURIDAD Y PROTECCIÓN DE USUARIOS Y CONSUMIDORES
4. PROMOCIÓN Y FORTALECIMIENTO DE LA COOPERACIÓN INTERNACIONAL ENTRE LOS ESTADOS PARA PREVENIR, PERSEGUIR, INVESTIGAR Y JUZGAR DE MANERA EFECTIVA LOS DELITOS CIBERNÉTICOS
5. PROMOCIÓN DE LA ASISTENCIA TÉCNICA, PROGRAMAS, PROYECTOS Y TRANSFERENCIA DE CAPACIDADES Y EXPERIENCIAS EN LA PREVENCIÓN DEL CIBERDELITO, EN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN
6. APOYO A LOS DEBATES EN LAS NACIONES UNIDAS Y OTROS FOROS MUNDIALES Y REGIONALES SOBRE LAS AMENAZAS EXISTENTES Y EMERGENTES, EL DESARROLLO Y LA IMPLEMENTACIÓN DEL MARCO PARA EL COMPORTAMIENTO DEL ESTADO RESPONSABLE EN EL CIBERESPACIO
7. FORTALECIMIENTO DE LA ARTICULACIÓN CON EL SECTOR PRIVADO, LA ACADEMIA, LA SOCIEDAD CIVIL Y OTROS ACTORES

Este último punto es de suma relevancia para el esfuerzo que se está desarrollando en esta Hoja de Ruta de Ciberseguridad, la cual justamente convoca a un modelo de trabajo concreto entre los distintos actores del ecosistema.

Esta declaración de la Cumbre de las Américas está de igual manera alineada con la Agenda Digital para América Latina y el Caribe (eLAC2020), la cual tiene como uno de sus objetivos: "Prevenir y combatir el cibercrimen mediante políticas públicas y estrategias de seguridad digital, el desarrollo y/o establecimiento de marcos normativos, el fortalecimiento de capacidades y la coordinación local, regional e internacional entre equipos de respuesta a incidentes informáticos" (Objetivo 24 eLAC2020, 2020). **Ambas agendas buscan transformarse en instrumentos catalizadores de los esfuerzos de cooperación regional en materia digital y de promoción del diseño de políticas, dentro de las cuales se incorpora la ciberseguridad como eje relevante.**

En el informe Ciberseguridad, Riesgos, Avances y el Camino a Seguir En América Latina y El Caribe, del BID, se destaca la importancia de contar con una estrategia nacional de ciberseguridad. Tal y como se menciona, "Hasta principios de 2020, solamente 12 países habían aprobado una estrategia nacional de ciberseguridad (un aumento con respecto a los 5 que tenían este tipo de estrategias en 2016), y únicamente 10 países han establecido un organismo gubernamental central responsable de la gestión de la ciberseguridad" (BID, 2020). **Chile es uno de los países que cuenta actualmente con una estrategia y agenda de ciberseguridad.**

En esta línea, es fundamental que los esfuerzos se realicen no sólo de forma individual por parte de las instituciones, sino que exista así mismo una estrategia nacional de ciberseguridad orquestada.

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Se han realizado diversos esfuerzos durante los últimos años por empujar distintos principios y directrices estratégicas de la ciberseguridad. En particular, en junio de 2022 se publicó la Hoja de Ruta de Transformación Digital para Chile 2035, propuesta desarrollada por la Comisión de Transportes y Telecomunicaciones del Senado, con el apoyo de la Comisión Económica para América Latina y el Caribe (CEPAL), la Asociación de Empresas de Telecomunicaciones (Chile Telcos) y la Cámara Chilena de Infraestructura Digital. Con ella se busca, de acuerdo a su propia definición, que Chile pueda "establecer políticas y medios que permitan la protección de sus activos informáticos y de comunicaciones, así como la resiliencia frente a eventuales vulnerabilidades o fallas" (Estrategia Transformación Digital Chile 2035, 2022).

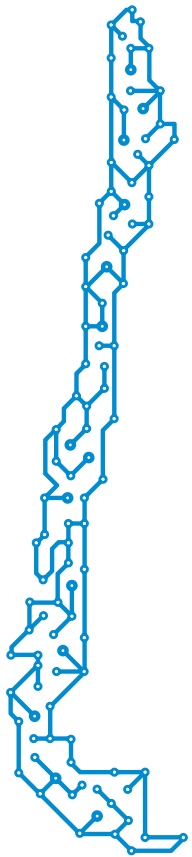
La Estrategia de Transformación Digital 2035 define dos grandes pilares: un Chile conectado sin brechas y un Chile digitalizado. Bajo estas directrices se encuentran siete componentes: Infraestructura digital habilitante; Desarrollo de habilidades digitales; Derechos digitales; Digitalización de la economía; Digitalización del Estado; Gobernanza y **Ciberseguridad**. Dentro de este último punto se plantea la **Propuesta de Estrategia 2035** con un modelo de tres horizontes proyectados a uno, cuatro y doce años, y cuenta con cincuenta iniciativas o propuestas de acción que declaran cumplir con **cinco grandes objetivos:**

1. Establecer un ecosistema de ciberseguridad nacional dinámico, robusto y resiliente
2. Desarrollar una cultura integral de ciberseguridad nacional
3. Gestión de talento, desarrollo de capacidades y de industria de ciberseguridad
4. Desarrollo de marcos legales y regulatorios efectivos y dinámicos, protección de derechos en ciberseguridad y persecución del cibercrimen
5. Cooperación internacional y liderazgo regional en ciberseguridad

Dentro de estos cinco grandes objetivos, las propuestas buscan que al año 2035 se puedan cumplir las siguientes metas o métricas de éxito tangibles de la política (Estrategia Transformación Digital Chile 2035, 2022):

1. Creación del Instituto Nacional de Ciberseguridad y del Centro de Capacidades de Ciberseguridad de Iberoamérica al 2023.
2. Creación de las nuevas agencias nacionales de Protección de Datos Personales y de Ciberseguridad y Protección de Infraestructura Críticas de la Información al 2025.
3. Creación de la totalidad de los CSIRT sectoriales y COC Nacional al 2030.
4. Inversión del gasto en I+D+i de Ciberseguridad como porcentaje del PIB en un 0,1% al 2025 y en 0,2% al 2030.
5. Formación de 10.000 profesionales certificados en Ciberseguridad al 2035, donde al menos el 30% de ellas sean mujeres.
6. 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.

Esta definición estratégica de transformación digital, y de ciberseguridad en particular, da cuenta de que actualmente **existe un diagnóstico estratégico claro asociado a las brechas y oportunidades en ciberseguridad** para Chile. Así mismo, existe una definición estratégica nacional de las líneas de intervención necesarias para avanzar en el nivel de madurez de ciberseguridad y, adicionalmente, se cuenta con un nivel de madurez cuantificado y un benchmarking regional e internacional sobre el cual ya se han establecido metas de crecimiento en los próximos doce años.



Por otro lado, los esfuerzos estratégicos también se ven complementados con **apoyos de organizaciones internacionales**, como el Banco Interamericano de Desarrollo, que cuenta con un portafolio de iniciativas para el fortalecimiento del ecosistema de ciberseguridad en el Cono Sur. En particular, **en Chile se han destinado recursos para fortalecer la capacidad del Ministerio del Interior y Seguridad Pública de gestionar incidentes cibernéticos a través de inversiones en infraestructuras tecnológicas, capacitación y sensibilización.**

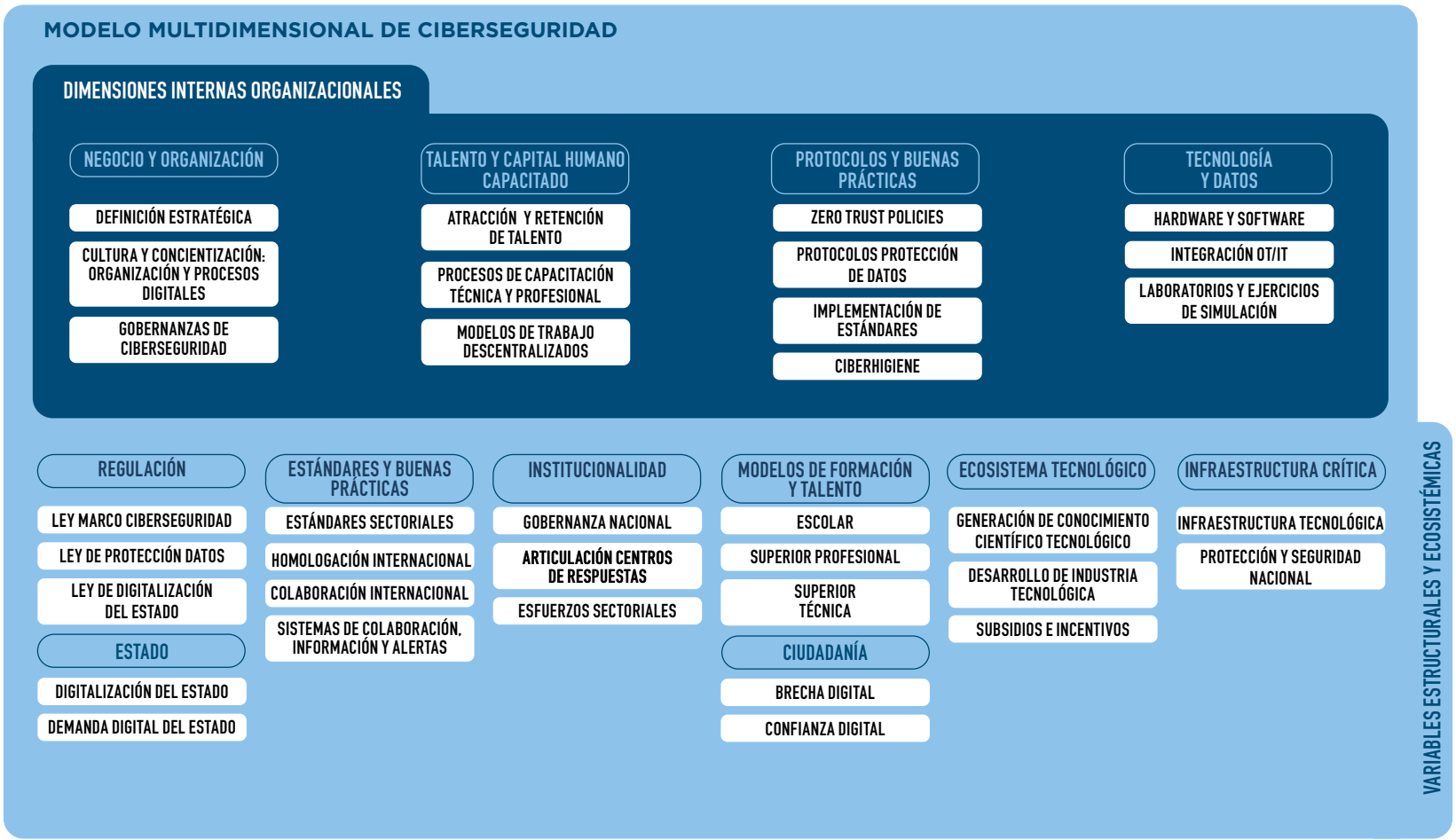
El Programa de Fortalecimiento de la Gestión Estratégica de la Seguridad Pública en Chile busca contribuir a la prevención de la violencia, la reducción del delito, incorporando un componente específico de financiamiento para la mejora de la capacidad de gestión de los delitos e incidentes cibernéticos en Chile. El financiamiento total se traduce en un apoyo de 96 millones de dólares, cuyo componente de ciberseguridad corresponde a 27 millones de dólares (BID, 2022).

El desafío para esta Hoja de Ruta es tener un enfoque práctico en este sentido, debe tener un foco táctico y empujar hacia el desarrollo de un plan de trabajo concreto durante los tres primeros años de implementación.
Este esfuerzo de focalización está alineado con el trabajo que se encuentra desarrollando la mesa temática "Ciberseguridad", convocada por la Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación del Senado, cuyo objetivo es crear las instancias de discusión y difusión necesarias para la ciberseguridad, al alero de la implementación de la Estrategia de Transformación Digital 2035.

La ejecución de esta definición táctica debe, por supuesto, responder a una priorización de dimensiones de trabajo que permita focalizar los esfuerzos en las líneas de mayor impacto durante los primeros tres años. En la próxima sección se analizarán brevemente las principales áreas de intervención propuestas para la discusión y priorización.

LA CIBERSEGURIDAD: PROBLEMA MULTIDIMENSIONAL ÁREAS DE INTERVENCIÓN

Considerando los antecedentes previos, la ciberseguridad se visualiza como un problema multidimensional con diversas áreas de intervención potencial. Este mapa inicial de áreas de interés se desarrolló en base a las entrevistas realizadas a más de veinte miembros del Comité Asesor, sumando a expertos de diversas áreas asociadas a la ciberseguridad.



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

El modelo base presenta cuatro áreas internas organizacionales, considerando la dimensión de las estrategias de ciberseguridad internas, que toman en cuenta la importancia de los nuevos modelos de negocios digitales, las tomas de decisiones basadas en datos, y cómo la cultura organizacional y los procesos internos deben adaptarse. Todos estos elementos abren espacios para la exposición a la ciberseguridad.

Por otra parte, la ejecución digital a nivel general, y más aún en el área de transformación digital y ciberseguridad, presenta siempre una brecha en talento y capital humano: ¿cómo atraer nuevo talento calificado? ¿cómo capacitar a nuestros colaboradores? son temáticas críticas que las organizaciones están buscando resolver. Y, finalmente, áreas internas asociadas a la implementación de protocolos, buenas prácticas y definición de inversión tecnológica e integración de sistemas a un nivel mucho más técnico.

Si bien todo lo anteriormente mencionado se puede encontrar en una organización, hay que estar conscientes de que, si el impacto que se quiere lograr está enfocado en la competitividad del país, en reactivación económica y bienestar, **el éxito de la implementación de ciberseguridad no está dado por el esfuerzo aislado de una única organización y mucho menos en una única área interna.** Las instituciones o compañías están insertas en un ecosistema y se ven influenciadas por variables estructurales y ecosistémicas relevantes que dependen de la intervención de otros actores del sistema local, regional e internacional.

En esta línea es donde las dimensiones asociadas a la infraestructura crítica nacional, los modelos de formación y talento disponibles tanto a niveles escolares, técnico, superior y de formación cívica comienzan a tomar protagonismo y relevancia. En esta misma directriz, **desde el Estado se plantea un rol fundamental asociado no sólo a lo regulatorio, sino también a su proceso de digitalización y a la institucionalidad y gobernanza de la ciberseguridad en el país.** Todo esto se engloba en el ecosistema y se ve influenciado por el nivel de desarrollo de la industria, del establecimiento de estándares y de la generación de buenas prácticas industriales que son fundamentales para el desarrollo de la ciberseguridad en su globalidad.

0.3 METODOLOGÍA

METODOLOGÍA Y MODELO CONCEPTUAL

El valor de construir esta Hoja de Ruta reside en su proceso, ya que permite unificar problemáticas comunes en torno a un diálogo intersectorial, que conduce a la elaboración de paquetes de trabajo que puedan ejecutarse a nivel país en los próximos 3 años.

El proyecto de esta Hoja de Ruta contó con dos instancias de interacción, en las cuales participaron activamente alrededor de cien profesionales, en dos instancias:

- El Comité Asesor fue integrado por directores y gerentes de grandes empresas del país, además de representantes del sector público y la academia. Su objetivo fue establecer las bases de una visión preliminar de la problemática, instaurando una mirada estratégica para desarrollar las áreas y brechas correspondientes a cada uno de los Comités de Desarrollo.

- Los Comités de Desarrollo fueron integrados por representantes de diversas organizaciones, que cuentan con experiencias en iniciativas privadas y públicas asociadas a las áreas detectadas. Por esta razón, existe un Comité por cada área priorizada con el objetivo de instaurar una mirada táctica y operativa por medio de la propuesta de proyectos concretos a implementar: Cultura, Talento y Tecnología.

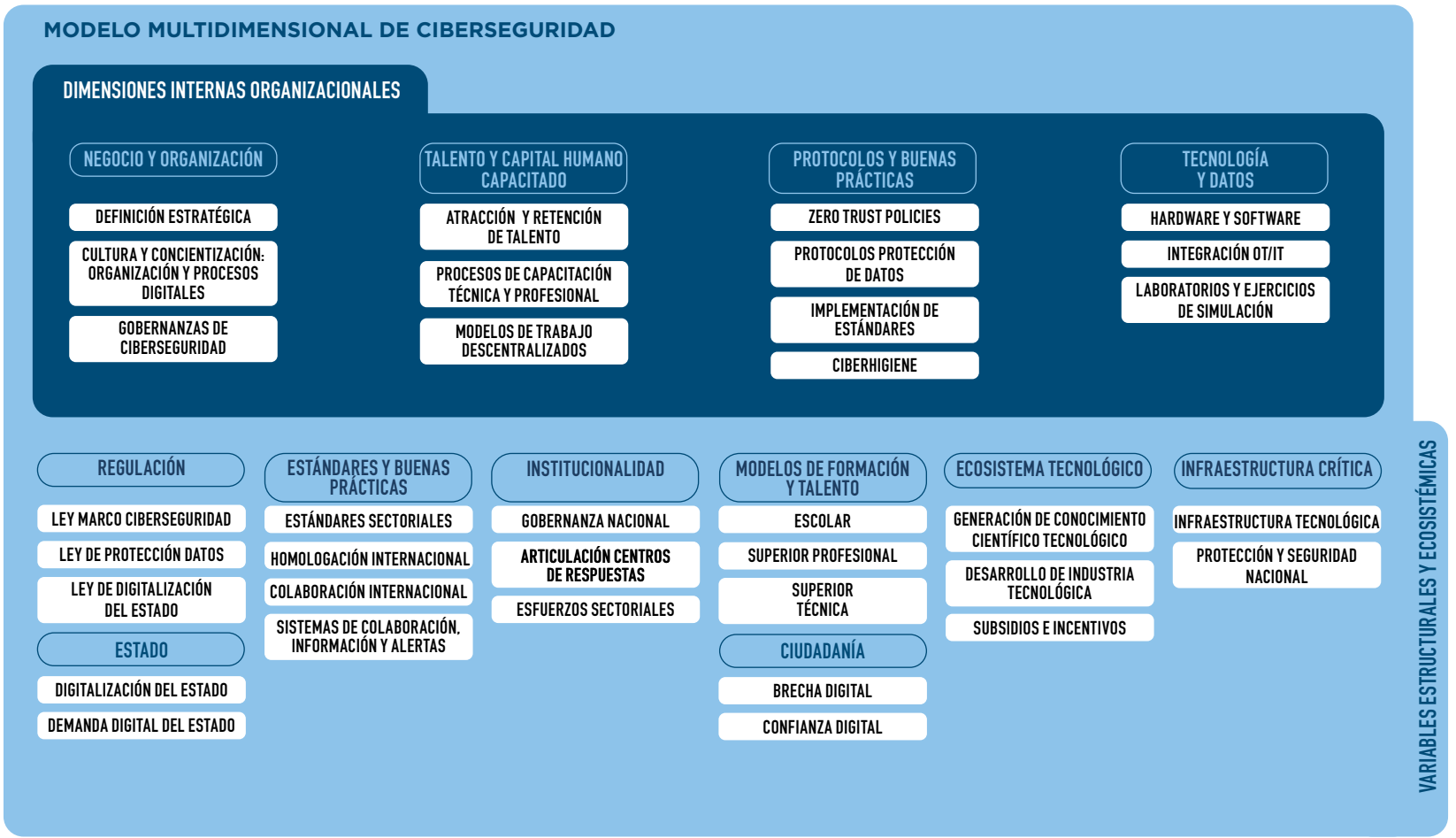
Inicialmente, el equipo ejecutivo de la Hoja de Ruta trabajó junto al Comité Asesor en la construcción de un diagnóstico sobre el estado de la ciberseguridad en Chile, lo que derivó en la definición de doce áreas. Este trabajo consistió en levantar la visión común de los distintos participantes del Comité Asesor a través de una revisión del estado del arte y la realización de más de 20 entrevistas semi-estructuradas a los miembros del Comité y otros profesionales relevantes por su conocimiento técnico del área. Desde una mirada estratégica, el Comité Asesor priorizó tres de las doce áreas de intervención, que dieron origen a los Comités de Desarrollo. Con la formación de ellos, se pretendió sumar más actores del ecosistema en línea con el espíritu colaborativo y la mirada país del proyecto. Una vez concluidas las sesiones de trabajo de los Comités de Desarrollo, el Comité Asesor adoptó un rol de análisis y priorización de los proyectos propuestos.

Esta Hoja de Ruta 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.

Los **resultados del proceso de elaboración de este documento** se componen de **tres elementos.**

1. **Diagnóstico compartido con brechas y oportunidades**. En este punto **se revisó qué experiencias comparadas existen, qué iniciativas se están ejecutando y cuáles son los lineamientos principales** que están empujando diversas instituciones involucradas en la materia. La captura de datos se realizó mediante el levantamiento del estado del arte y entrevistas en profundidad a integrantes del Comité Asesor y actores claves del ecosistema.

De este barrido **se identificaron doce áreas estratégicas relevantes** tanto a nivel de dimensiones internas organizacionales (como los protocolos y buenas prácticas, junto con las tecnologías y el negocio), como a nivel de variables estructurales y ecosistema, pasando por el desarrollo de infraestructura crítica hasta el desarrollo de un ecosistema científico, tecnológico y de financiamiento. (Figura 1).



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

② **Priorización estratégica de las líneas de trabajo críticas.** Se definieron tres áreas de trabajo prioritarias: (1) Área de Talento y Desarrollo de Competencias para la ciberseguridad; (2) Área de Cultura en Ciberseguridad y; (3) Área de Tecnología, Protocolos, Estándares y Ecosistema.

Ese proceso dio pie a la creación de tres Comités de Desarrollo. Cada uno de ellos desarrolló portafolios de proyectos atingentes a las brechas detectadas en cada área.

③ **Portafolio de proyectos públicos y privados**, que consideran un horizonte de trabajo de tres años, acompañados de los principales hitos e indicadores de éxito que se deben desarrollar de forma crítica para sentar las bases necesarias para alcanzar la visión de futuro de esta Hoja de Ruta. (Figura 3).

ÁREAS PRIORIZADAS DEL MODELO MULTIDIMENSIONAL DE CIBERSEGURIDAD.

TALENTO Y COMPETENCIAS EN CIBERSEGURIDAD

- ATRACCIÓN Y RETENCIÓN DE TALENTO
- MODELOS DE TRABAJO DESCENTRALIZADOS
- ESCOLAR
- SUPERIOR TÉCNICA
- SUPERIOR PROFESIONAL
- MODELOS DE CERTIFICACIÓN DE CAPACIDADES
- CAPITAL HUMANO AVANZADO

TECNOLOGÍA Y ECOSISTEMA, PROTOCOLOS Y ESTÁNDARES EN CIBERSEGURIDAD

- ZERO TRUST POLICIES
- PROTOCOLOS DE PROTECCIÓN DE DATOS
- IMPLEMENTACIÓN DE ESTÁNDARES
- HOMOLOGACIÓN INTERNACIONAL
- SISTEMAS DE COLABORACIÓN, INFORMACIÓN Y ALERTAS
- HARDWARE Y SOFTWARE
- INTEGRACIÓN OT/IT
- EJERCICIOS DE SIMULACIÓN Y SANDBOXES
- GENERACIÓN DE CONOCIMIENTO CIENTÍFICO TECNOLÓGICO
- SUBSIDIOS E INCENTIVOS

CULTURA CIBERSEGURIDAD

- DEFINICIÓN ESTRATÉGICA
- CULTURA Y CONCIENTIZACIÓN: ORGANIZACIÓN Y PROCESOS DIGITALES
- ESFUERZOS SECTORIALES
- CIBERHIGIENE
- CIUDADANÍA

Fuente: Elaboración propia equipo Hoja de Ruta de Ciberseguridad 2022

HITOS DE TRABAJO

ABRIL 2022

SESIÓN 1 DEL COMITÉ ASESOR

- Presentación de integrantes
- Definición de una visión audaz de futuro

MAYO

ENTREVISTAS 1 A 1

- Levantamiento de visiones de representantes del ecosistema respecto a brechas y oportunidades para la ciberseguridad
- Levantamiento del estado del arte

JUNIO

SESIÓN 2 DEL COMITÉ ASESOR

Diagnóstico y áreas estratégicas

- Presentación de diagnóstico compartido
- Priorización de áreas temáticas para los Comités de Desarrollo

JULIO

KICK-OFF

COMITÉS DE DESARROLLO

Presentación miembros Comité Visión audaz de futuro

AGOSTO

SESIÓN 1 COMITÉS DE DESARROLLO

Definición dimensiones impacto e indicadores

Dimensiones de impacto

- Indicadores de desempeño notable

AGOSTO

SESIÓN 2 COMITÉS

Desarrollo divergencia de proyectos

Propuestas de proyectos para cada uno de los indicadores de desempeño notables definidos

SEPTIEMBRE

SESIÓN 3 COMITÉS DE DESARROLLO

Convergencia de proyectos

Definición de horizontes de trabajo, alcance e impacto de los proyectos

SEPTIEMBRE

SESIÓN 4 COMITÉS DE DESARROLLO

Priorización proyectos

- Priorización de proyectos
- Consolidación de Portafolios

OCTUBRE

SESIÓN EXTRAORDINARIA COMITÉ ASESOR

- Ejecución ágil de proyectos propuestos: Piloto de Academia de Ciberseguridad (Microsoft-UC)

OCTUBRE

SESIÓN FINAL COMITÉ ASESOR

Presentación portafolio y priorización de paquetes de trabajo

DICIEMBRE 2022

LANZAMIENTO DEL DOCUMENTO HOJA DE RUTA DE CIBERSEGURIDAD + COMPROMISO DE EJECUCIÓN

- Ejecución ágil de proyectos propuestos: Certificación de pymes (Min. de Economía y Microsoft)

0.4
PRINCIPALES BRECHAS EN CIBERSEGURIDAD

Al considerar un plan de trabajo de tres años, nace la necesidad de priorizar las doce dimensiones y ecosistemas presentados en el proceso de creación de esta Hoja de Ruta. Es por eso que se ha realizado un esfuerzo por agruparlos y sintetizarlos en seis grandes dimensiones de intervención importantes a abordar y a priorizar:

1. Infraestructura crítica
2. Cultura de ciberseguridad
3. Talento y competencias
4. Protocolos y estándares
5. Tecnología y ecosistema
6. Áreas transversales asociadas a regulación, institucionalidad y Estado digital.

Cada una de estas dimensiones se pueden abordar y analizar tanto desde la perspectiva privada interna de las organizaciones, como a nivel estructural y de ecosistema, abriendo el espacio para discusiones intrasectoriales relevantes para el contexto de esta Hoja de Ruta. **En base a estas primeras seis áreas es que se discutieron las perspectivas estratégicas de cada una de ellas y se priorizaron las tres dimensiones más relevantes.** A continuación, se presenta una síntesis de cada una de las seis áreas:

1. INFRAESTRUCTURA CRÍTICA

De acuerdo a lo mencionado en el último estudio del Banco Interamericano de Desarrollo (BID, 2020) y el Informe de Riesgos Globales 2020 del Foro Económico Mundial (WEF, 2020), **se plantea el riesgo de ciberataques a la infraestructura crítica y el robo de datos entre los diez principales peligros con mayor probabilidad de ocurrir.** Este daño a la infraestructura crítica podría alcanzar incluso hasta el 6% del PIB (WEF en BID, 2020).

Respecto a qué tipo de infraestructura se considera como crítica, existen diversos enfoques y definiciones. En términos generales, la información de sectores prioritarios y regulados como **energía, telecomunicaciones, servicios sanitarios, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa, entre otras, pueden considerarse como parte de las líneas críticas establecidas** (BID, 2020). En el Proyecto de Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información, se define el concepto de infraestructura crítica como "aquellas instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación de servicio, interceptación, interrupción o destrucción puede tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que éste debe proveer o garantizar." (Senado, 2022). Esta definición es interesante desde el punto de vista de la integración de los conceptos de infraestructura física e infraestructura de la información, como parte de un sistema crítico de funcionamiento de las redes nacionales.

Uno de los principales puntos asociados a las redes críticas es su protección y la implementación de un sistema resiliente de conectividad. De acuerdo a la Subsecretaría de Telecomunicaciones de Chile, al menos al momento de la revisión en 2017-2018, existían 12.186 sitios declarados críticos de redes móviles. Hoy en día, en Chile existen alrededor de 30.000 antenas y la llegada del 5G aportará con 9.000 más, aproximadamente (Subtel, 2022). En un estudio de NICLabs para SUBTEL se estimó que la inversión necesaria para una red de fibra óptica resiliente para el 90% de la población costaría alrededor de 333 millones de pesos (NIC, 2019).

2. CULTURA DE CIBERSEGURIDAD

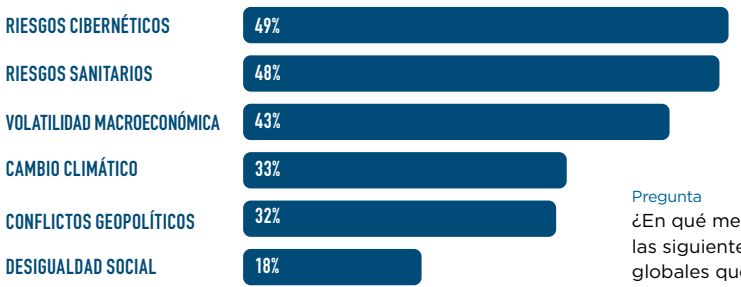
A pesar de los altos niveles de sofisticación tecnológica a los que se pueden llegar en temas de ciberseguridad, las cifras indican que el gran porcentaje de ataques provienen de acciones tan sencillas como contraseñas inseguras, o bien, vía correo electrónico. **Los estudios indican que la higiene básica de ciberseguridad, como el uso de antimalware, limitar privilegios de acceso, autenticaciones de identidad con multifactor, protección de datos y actualizaciones de sistema, previenen un 98% de los ataques** (Microsoft, 2021). Estas cifras dan cuenta de la relevancia de los programas de concientización de los colaboradores en cuanto a procesos digitales y a higiene digital. Esta dimensión es crítica, considerando que la tecnología de ciberseguridad y su impacto en los procesos de negocios sólo tendrán un efecto si la implementación por parte de los operadores y colaboradores de la organización está alineada con un comportamiento responsable.

SEGURIDAD DE LA INFRAESTRUCTURA:
ZERO TRUST

- Tratar cada intento de acceso como si se originara de una red no confiable.
- Eliminar dispositivos desconocidos o no manejados. Identidad como servcio.

Además, **es fundamental que estas preocupaciones a nivel cultural provengan así mismo de los directorios y altas gerencias de las empresas,** definiendo la ciberseguridad a nivel basal como uno de los elementos estratégicos de las organizaciones. Esta dimensión también pasa por relevar la importancia de los planes de capacitación para altos directivos y profesionales que lideran organizaciones y la toma de decisiones estratégicas. Esta tendencia se puede ver en la última encuesta de PwC, que caracteriza cómo los directores están considerando prioritarios los riesgos cibernéticos, como amenazas para el crecimiento del negocio.

DIRECTORES EJECUTIVOS CLASIFICAN LOS RIESGOS CIBERNÉTICOS COMO LA PRINCIPAL AMENAZA PARA EL CRECIMIENTO, SEGUIDOS DE CERCA POR LOS RIESGOS SANITARIOS



Pregunta
¿En qué medida le preocupan las siguientes amenazas globales que afectarán negativamente a su empresa en los próximos 12 meses?

(Se muestran sólo las respuestas "muy preocupado" y "extremadamente preocupado")

Fuente: 25ª Encuesta Anual de CEOs de PwC

Considerando en términos mucho más amplios de la ciudadanía, una cifra preocupante en este punto es que, de acuerdo al estudio "Iceberg Digital" de Kaspersky (2020) para Latinoamérica, existen brechas culturales básicas sumamente notorias en los países de la región. Por ejemplo, **el 49% de los latinoamericanos no resguarda los datos que actualmente almacena en la nube porque no sabe cómo hacerlo o porque desconoce que esta plataforma debe protegerse de eventuales robos o ciberataques", siendo Chile el segundo país que menos protege la información personal de la nube, con un 53%.** Así mismo, al consultar a los encuestados por temas relativos al Internet de las Cosas (IoT), un 46% ignora que sus dispositivos conectados pueden ser hackeados a través del router y un 25% desconoce cómo funciona este tipo de tecnología. (Kaspersky, 2020; Pwc, 2020). Este tipo de brechas, se agudizan aún más si se desagregan los análisis considerando variables demográficas, afectando en mayor proporción a mujeres, personas mayores, y la población de menores ingresos y menor nivel educacional (SUBTEL, 2021).

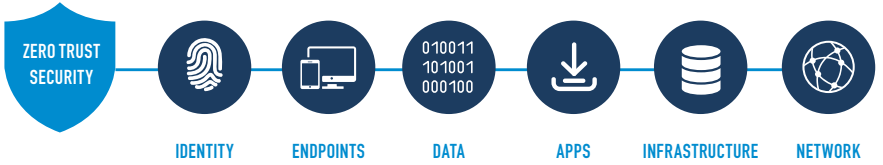
Estos antecedentes dan cuenta de la relevancia del desarrollo de una cultura digital para abordar no sólo el comportamiento de los colaboradores y líderes dentro de las organizaciones por medio de la adopción de mejores prácticas de prevención de ataques, sino también las brechas digitales en la ciudadanía, de cara a un aumento progresivo en la exposición a interacciones digitales, con empresas privadas y con los servicios del Estado.

3. PROTOCOLOS, ESTÁNDARES Y BUENAS PRÁCTICAS

Muy alineado con el desarrollo cultural está la adopción de protocolos y mejores prácticas de la industria para prevenir las brechas de seguridad más recurrentes. Si bien existen diversos protocolos, el más aceptado como línea base es la política de "Zero Trust o confianza cero", la cual declara que está diseñada para proteger los entornos modernos, tomando como principio base eliminar la confianza implícita en las interacciones digitales de la organización y validar continuamente cada etapa de una interacción **(PaloAlto Networks, 2022).**

Un esfuerzo importante respecto a implementación de esfuerzos sectoriales técnicos es el que está desarrollando el Coordinador Eléctrico Nacional, quien por encargo de la Superintendencia de Electricidad y Combustibles (SEC), desde 2019 aproximadamente se encuentra en un proceso de facilitación de la adopción de una adaptación local de las normas NERC-CIP, estándar de ciberseguridad aplicado a compañías del sistema eléctrico, actualmente utilizado en Estados Unidos, y que al día de hoy está en más de un 60% de adopción a nivel general de la industria (CEN, 2022).

Este tipo de adopciones de estándares industriales apoyan la transición hacia los cambios regulatorios y de certificaciones necesarios para acompañar la madurez de las dinámicas de la industria. Además, pueden ser replicados en otros sectores menos estandarizados. A nivel sectorial, gremios como la ACTI y la AMCHAM se encuentran realizando esfuerzos relevantes para difundir las mejores buenas prácticas entre sus asociados de la industria.



Fuente: "What is Zero Trust?", Microsoft.

QUÉ ES CERT

CERT es un término protegido y registrado en Estados Unidos por el CERT-CC.
Dependiendo del país, los equipos pueden tener distintas denominaciones, como CSIRT, CIRT y SIRT, entre otras.

Fuente: Programa de Ciberseguridad OEA/CICTE

4. TALENTO

La alta escasez de capital humano y talento especializado en temas de ciberseguridad es una realidad actual dentro y fuera de Chile. De acuerdo a Microsoft, **"para 2025, habrá 3,5 millones de empleos de ciberseguridad abiertos en todo el mundo, lo que representa un aumento del 350% en un período de ocho años"** (2020). Es por eso que ya a nivel privado se están impulsando iniciativas para fomentar la formación y certificación en esta área. Un ejemplo concreto es la alianza de Microsoft con Women in Cybersecurity, una ONG que fomenta el reclutamiento, retención y promoción de mujeres en ciberseguridad (Microsoft, 2020) o Programas de Certificación no convencionales como la iniciativa Escuela 42 de Telefónica, un "campus de programación 42 es gratuito, presencial y está abierto a todo tipo de talento, sin necesidad de titulaciones ni estudios previos", que se encuentra presente ya en más de veinte países (Fundación Telefónica, 2021).

HABILIDADES Y TALENTOS ACTUALMENTE DISPONIBLES PARA QUE CIBER-LÍDERES ENFRENTEN CIBERATAQUES

Fuente: Global Cybersecurity OUTLOOK 2022

Dentro del ecosistema nacional, también existen espacios de captura de talento relevantes en áreas afines. Por ejemplo, Chile cuenta con **Encuentros de Matemáticas** orientados a estudiantes desde hace más de treinta años, instancias de alto valor para la retención y captura de talento joven. La Sociedad de Matemática de Chile organiza en particular la **Olimpiada Nacional,** un programa que cuenta con más de treinta y dos años de experiencia, con un alcance en todas las regiones de más de doce mil participantes al año. Así mismo, desde 2011 la Facultad de Matemáticas UC organiza un programa de dos años de duración, orientado a estudiantes de segundo y tercero medio, llamado Taller de **Razonamiento Matemático** que recibe más de 650 estudiantes al año. Adicionalmente, junto al apoyo de la Fundación Impulso Inicial y la Facultad de Matemáticas UC, Chile comenzó a participar de **competencias matemáticas dirigidas a mujeres** (Facultad de Matemáticas UC, 2022).

Este tipo de esfuerzos también se complementan con ejercicios de ciberseguridad específicamente desarrollados para el área, como la iniciativa **Campo de Marte,** desarrollada desde 2018 con el apoyo del senador Kenneth Pugh, la Unidad del Ciber Crimen de Valparaíso y la Universidad Andrés Bello (Campo de Marte, s/f). Existen también esfuerzos públicos en Chile, como los realizados por el Ministerio de Economía, Fomento y Turismo, a través de sus servicios CORFO y SERCOTEC, que ofrecen cursos gratuitos para mipymes que enseñan ciberseguridad (CORFO 2022 y Sercotec 2022).

Un ejemplo internacional es el **programa estadounidense CyberCorps** que está diseñado para reclutar y capacitar a la próxima generación de profesionales de TI para satisfacer las necesidades de ciberseguridad de Estados Unidos. Esta iniciativa ofrece becas para la educación de pregrado y posgrado (MS o PhD) en ciberseguridad. Las asignaciones se financian a través de subvenciones otorgadas por la Fundación Nacional de Ciencias (NSF). A cambio del financiamiento de sus estudios, los beneficiarios deben aceptar trabajar para el Gobierno de los EE. UU. después de graduarse, en un cargo relacionado con la ciberseguridad, por un período igual a la duración de la beca (U.S. Department of Homeland Security, 2022).

En términos de oferta de formación profesional, también existen iniciativas como el **programa de estudios de Maestría en Ciberseguridad,** desarrollado por el BID y el grupo Computer Security Lab (COSEC) de la Universidad Carlos III de Madrid (U3CM). Este programa de estudio, presentado el 2021, es de uso libre y gratuito, orientado a las universidades de la región de América Latina y el Caribe. Además, cuenta con la documentación asociada a la malla de estudios, la fundamentación técnica, metodologías docentes sugeridas, perfiles de ingreso y egreso, así como los planes de admisión y lanzamiento del programa, de manera tal que brinda a las universidades todas las herramientas de implementación prácticas necesarias para la generación de este nuevo programa de formación (BID, 2021).

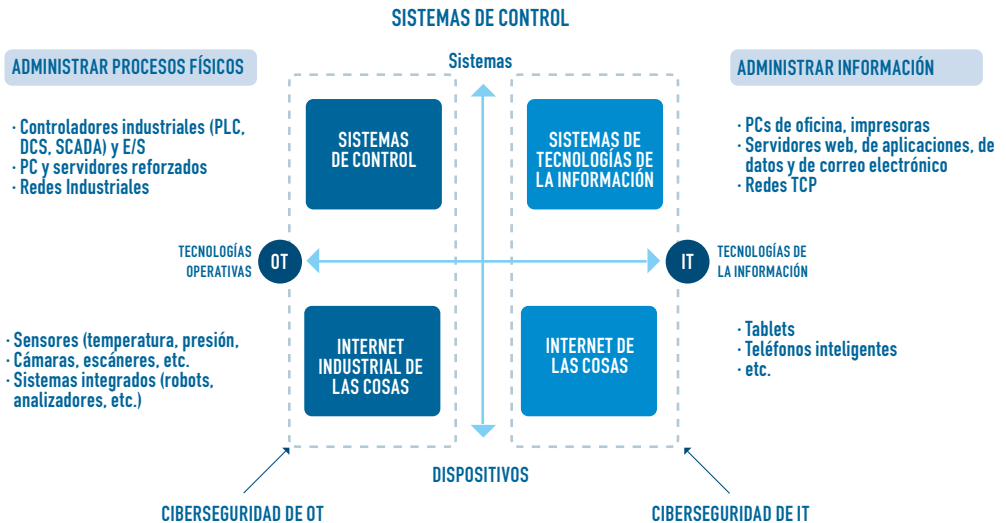
5. TECNOLOGÍA Y ECOSISTEMAS

De acuerdo a Mckinsey, una de las principales tendencias hoy en día es la adopción tecnológica por parte de los hackers, quienes actualmente utilizan herramientas como inteligencia artificial, Machine Learning y otras tecnologías para lanzar ataques cada vez más sofisticados. Esto ha hecho más eficientes, de menor costo y más efectivos muchas de estas acciones, llegando el ciber hackeo a ser una industria de 300 mil millones de dólares. (InsureTrust, 2019; Mckinsey, 2022).

Este escenario genera una presión importante en el ecosistema susceptible a este tipo de ofensivas, dado que se da cuenta de que **"la gestión del riesgo cibernético no ha seguido el ritmo de la proliferación de transformaciones digitales y analíticas, y muchas empresas no están seguras de cómo identificar y gestionar los riesgos digitales".** (McKinsey, 2020). Este punto también es fundamental cuando se analizan los desafíos asociados a integración OT (tecnologías operativas) e IT (tecnologías de la información) que viven las organizaciones. Por esto es crítico para las organizaciones la incorporación y adopción de tecnología, de la mano de un cambio cultural adecuado e implementación de protocolos y buenas prácticas.

Tan sólo **a nivel de tecnología, la adopción de inteligencia artificial, el análisis de seguridad y la encriptación fueron los tres factores críticos para mitigar y reducir el costo de un ciberataque.** Se ha estimado que las empresas que adoptan estas tecnologías han ahorrado entre $1.25 millones y $1.49 millones de dólares. (IBM Corporation, 2021).

CONVERGENCIA E INTEGRACIÓN OT/IT



En esta línea, el mercado global de ciberseguridad tendrá un valor de 403 mil millones de dólares para 2027 con una tasa de crecimiento anual compuesto (CAGR) del 12,5%, según Brand Essence Research. El estudio afirma que el mercado de la ciberseguridad tenía un valor de 176.5 mil millones de dólares en 2020 y se sigue previendo un crecimiento importante. (Brand Essence Research, 2021).

Existen múltiples becas y subsidios del sector público en desarrollo de capital humano, nuevas tecnologías y proyectos relacionados a la ciberseguridad. Por ejemplo, la Unión Europea en el año 2020 concedió 49 millones de euros para impulsar la innovación en los sistemas de ciberseguridad y privacidad (European Commission, 2020). El punto fundamental en este caso es entender la necesidad de la adopción tecnológica de la mano de equipos técnicos especializados, que permitan realizar una vigilancia y desarrollo tecnológico de acuerdo a la evolución de los ataques que ocurren en el ecosistema internacional.

6. ÁREAS TRANSVERSALES: REGULACIÓN, INSTITUCIONALIDAD Y ESTADO DIGITAL

En los indicadores de madurez de ciberseguridad se menciona que una de las dimensiones de mayor desarrollo a nivel nacional es la dimensión regulatoria. En esta línea, actualmente existen diversos marcos regulatorios relevantes en la materia, cada uno en distintos niveles de implementación. Algunos de los más relevantes son:

1. LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN

Hoy en día, a nivel de gobernanza, existe la figura del Comité Interministerial de Ciberseguridad, que cumple el rol de asesorar al Presidente de la República en el análisis e implementación de la Política Nacional de Ciberseguridad y otras medidas asociadas al área.

En marzo de 2022, se ingresó a tramitación en el Senado el proyecto de ley que establece **una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.** Este proyecto tiene un fuerte enfoque institucional y de gobernanza que, de acuerdo al mismo documento, busca "Establecer la institucionalidad, los principios y la normativa general que permiten estructurar, regular y coordinar las acciones de ciberseguridad de los órganos de la Administración del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los órganos del Estado así como los deberes de las instituciones privadas que posean infraestructura de la información calificada como crítica y, en ambos casos, los mecanismos de control, supervisión, y de responsabilidad por la infracción de la normativa." (Proyecto de Ley Marco Ciberseguridad, 2022).

En estos términos, la Ley Marco propuesta se construye sobre ocho principios rectores fundamentales: responsabilidad; protección integral, confidencialidad de los sistemas de información; integridad de los sistemas informáticos y de la información; disponibilidad de los sistemas de información; control de daños; cooperación con la autoridad y especialidad en la sanción. Cada uno de ellos puede verse en mayor detalle en el proyecto de ley.

La Ley Marco, adicionalmente propone la **creación de distintas instituciones con roles de articulación y orquestación de esfuerzos. Entre ellos, se destacan la creación de la Agencia Nacional de Ciberseguridad con su correspondiente Consejo Técnico,** así como la conformación del **Equipo Nacional de Respuesta a Incidentes de Seguridad Informática** (CSIRT Nacional), acompañado de equipos de respuesta a incidentes de seguridad informática sectoriales (CSIRT Sectoriales), un Equipo de Respuesta ante **Incidentes de Seguridad Informática del Sector Gobierno (CSIRT de Gobierno) y el Centro Coordinador del Equipo de Respuesta ante Incidentes de Seguridad Informáticos del Sector Defensa** (CSIRT Sectorial de Defensa), entre otros. Este proyecto de ley recoge puntos críticos asociados a la definición de infraestructura crítica y los pasos para la generación de una red de colaboración e institucionalidad robusta.

2.Ley de Delitos Informáticos

Este punto es sumamente crítico si se considera que, de acuerdo a la Brigada Investigadora del Cibercrimen (Bricib) Metropolitana, entre los años 2020 y 2021 se presentaron alzas de entre un 30% y un 45% de delitos cibernéticos, principalmente asociados a estafas, sabotaje informático o adquisición de material pornográfico infantil (PDI, 2022).

El 20 de junio de 2022, se promulgó la Ley número 21.459 que establece la nueva normativa de los delitos informáticos en Chile y permite las adecuaciones necesarias para aplicar al Convenio de Budapest. La ley considera la incorporación, por ejemplo, de delitos como el fraude informático, la receptación de datos informáticos o el acceso indebido a sistemas o datos, entre otros (Senado, 2022).

3.Ley de Protección de Datos Personales

Desde 2017, se encuentra ingresado el Proyecto de Ley de Protección de Datos y el Tratamiento de los Datos Personales, que propone la actualización de la antigua ley N° 19.628 sobre Protección de la Vida Privada, redefiniendo los principales estándares de tratamiento de datos de acuerdo a estándares y compromisos internacionales. Así mismo, se propone la creación de la Agencia de Protección de Datos Personales como autoridad de control. (Senado, 2022). Este marco de trabajo es igualmente relevante en términos de las potenciales brechas de información a las que pueden quedar expuestos tanto datos públicos como privados. Esta ley se encuentra actualmente en segundo trámite constitucional en la Cámara de Diputadas y Diputados.

4.Ley Transformación Digital del Estado

Un elemento relevante en la discusión es el papel que cumple el Estado como garante de la seguridad de la información de la ciudadanía y en su rol de demandante de soluciones y servicios de ciberseguridad, o bien, con estándares altos de ciberseguridad, según corresponda.

En esta línea, es fundamental reconocer que desde 2019 la Ley N° 21.180 de Transformación Digital del Estado modifica las bases de los procedimientos administrativos y establece que "Todo procedimiento administrativo deberá expresarse a través de los medios electrónicos establecidos por ley, salvo las excepciones legales" (Ley 21.280, 2019). Esto tiene como objeto dar mayor transparencia, trazabilidad y velocidad al sistema público. Sin embargo, se deben considerar los desafíos asociados a la protección de datos personales y a la robustez de los sistemas de datos y procesamiento con los que deben contar los distintos cuerpos del Estado para cumplir con esta materia. Se definieron cinco años para la implementación de todos sus reglamentos, desde la publicación de la ley, es decir, hasta el 2024. Esto, por supuesto, supone presiones por desarrollar un despliegue tecnológico y cultural digital que incorpore buenas prácticas de ciberseguridad.

5.Ley Mes de Ciberseguridad Octubre

Finalmente, dentro del contexto de iniciativas específicas de ciberseguridad, desde 2018 la Ley 21.113 declara el mes de octubre de cada año como el "Mes Nacional de la Ciberseguridad", homologando la efeméride que existe en Estados Unidos y Europa. Esta iniciativa busca el fomento de actividades de concientización y promoción de la ciberseguridad en el país.

Así mismo, de forma complementaria existe actualmente una propuesta de proyecto para definir el mes de noviembre como Mes Nacional de la Infraestructura Crítica y su Resiliencia (Senado de Chile, 2022).

0.5
TRABAJO DE LOS COMITÉS DE DESARROLLO

De las dimensiones descritas anteriormente, el Comité Asesor priorizó tres áreas que dieron origen a los Comités de Desarrollo: Talento y Desarrollo de Competencias para la ciberseguridad, Cultura para la ciberseguridad y Tecnología, ecosistema, protocolos y estándares para la ciberseguridad; los cuales comprenden una serie de subdimensiones descritas en capítulos previos, que se ven resumidas en el siguiente esquema.

ÁREAS PRIORIZADAS DEL MODELO MULTIDIMENSIONAL DE CIBERSEGURIDAD.

Fuente: Elaboración propia equipo Hoja de Ruta de Ciberseguridad 2022

COMITÉ DE DESARROLLO
TALENTO Y DESARROLLO DE COMPETENCIAS EN CIBERSEGURIDAD

El primer comité contempla los desafíos de formación de talento y competencias para la ciberseguridad, considerando nuevos modelos educativos, desde la formación básica y profesional hasta la reconversión laboral, así como la capacitación y certificación no-tradicional de competencias.

OBJETIVO

El objetivo de esta mesa de trabajo fue desarrollar el diseño y propuestas de implementación de un portafolio de iniciativas a nivel táctico, conteniendo proyectos de desarrollo privados, propuestas de política pública y/o de colaboración entre distintos sectores, enfocándose en las problemáticas asociadas al cierre de brechas de talento en ciberseguridad local.

Como línea base de discusión del Comité de Desarrollo de Talento y Competencias, se definió una visión de futuro audaz que refleja la imagen del cambio y del éxito que se visualiza para el país en los próximos años y el impacto que se aspira generar con las iniciativas propuestas.

Visión audaz de futuro

"Chile es un país ciberseguro, un polo de atracción y generación de talento inclusivo que, sin importar género ni estatus socioeconómico, disponibiliza y facilita el desarrollo de mecanismos de formación y reconversión en ciberseguridad para contar con el capital humano para proteger y defender la vida, la identidad y los activos de los ciudadanos y las instituciones".

OBJETIVOS ESPECÍFICOS E INDICADORES DE DESEMPEÑO NOTABLES

Con el fin de enmarcar y orientar el trabajo e impacto de los proyectos propuestos, se delimitaron siete objetivos de trabajo que describen el área de intervención declarada por este comité. Los objetivos están orientados a realizar desde el levantamiento y catastro de brechas en talento y perfiles, hasta el desarrollo de modelos de detección temprana de talento y acceso universal a capas de conocimiento fundamental de ciberseguridad, junto con modelos de financiamiento e incentivos a la generación de talento, entre otros. Cada uno de estos objetivos tiene métricas e indicadores de éxito claros que permiten hacer un seguimiento concreto del impacto que el portafolio generará en el ecosistema. A continuación, se presentan las tablas resúmenes de ambos puntos.

OBJETIVOS	INDICADORES
1 Definir línea base de roles y cargos que puedan necesitarse en el mercado de la ciberseguridad de forma transversal en toda la cadena de actividades y realizar el cruce con el tipo de certificación necesaria y las capacitaciones disponibles.	• # Cantidad de profesionales preparados al 2025 y que tributan a la meta de 10.000 profesionales al 2035 • % de profesionales certificados en competencias en ciberseguridad • % de profesionales reconvertidos hacia perfiles técnicos y profesionales requeridos en el ámbito de la ciberseguridad • # Cantidad de egresados de programas de educación superior técnica en el área de ciberseguridad
2 Levantar qué empresas tienen o tendrán obligación regulatoria, que requiere profesionales de ciberseguridad en Chile.	• Hito: Estudio de levantamiento de obligaciones regulatorias.
3 Desarrollar modelos de detección temprana de talento joven a nivel escolar de nivel básica y media.	• # Cantidad de estudiantes de educación escolar básica y media capacitados en competencias para la ciberseguridad. • # Cantidad de menores de 18 años con certificaciones en ciberseguridad logradas • % de talento temprano apadrinado por empresas
4 Desarrollar modelos de institucionalidad nacional para la ciberseguridad.	• Hito: Creación Instituto Ciberseguridad y gobernanza ciberseguridad
5 Desarrollar mecanismos de acceso universal a capas iniciales de ciberseguridad que permitan un ingreso laboral inicial en ciberseguridad.	• # de profesionales reconvertidos hacia perfiles técnicos y profesionales requeridos en el ámbito de la ciberseguridad
6 Incluir y descentralizar capacidades y talento para la ciberseguridad.	• % de mujeres que ocupen cargos y funciones relacionadas con la ciberseguridad • % de talento presente en regiones
7 Desarrollar modelos de financiamiento para la formación e investigación en ciberseguridad.	• % del presupuesto nacional destinado a formación en ciberseguridad

REFLEXIONES GENERALES DEL COMITÉ

Dentro de las conversaciones de la mesa de trabajo, se recalca la importancia de **poner el foco en el desarrollo transversal e interdisciplinario, no sólo de competencias técnicas TI, sino en todos los perfiles de talentos necesarios en toda la cadena de actividades.** Algunos referentes en esta línea fueron el *framework* de trabajo NICE que presenta siete grandes categorías de capas de la ciberseguridad, que se desglosan en 33 áreas de distinta especialidad. Esto da cuenta de la importancia de la formación en ciberseguridad fuera de las áreas de tecnologías y en el trabajo colaborativo transversal de las áreas de negocios, en cuanto a incorporar talento capacitado en ciberseguridad a sus operaciones.

En esta línea, dada la necesidad de especialización pero también de agilidad en la formación de perfiles, **se requieren nuevos sistemas o modelos educativos adaptados al *journey* de cada persona**. Esto implica flexibilizar los programas y modelos de certificación actuales, generando una apertura a modelos alternativos de formación y certificación de competencias críticas.

Finalmente, un tema que surge de forma transversal se refiere a **incorporar elementos de inclusión y transversalidad**, rescatando la perspectiva de generación de talento, sin importar género ni estatus socioeconómico, enfocándose en competencias y capacidades.

PROPUESTAS DE PROYECTOS

El portafolio de esta área se compone de **once iniciativas de talento y competencias,** enfocadas principalmente en **tres ejes de trabajo**. Por una parte, el **desarrollo de mecanismos e incentivos a la inversión en generación de talento,** cuyo foco es en la generación de mecanismos para facilitar que las organizaciones realicen inversiones en programas de talento en ciberseguridad y apoyen la formación de nuevos programas. Por otro lado, se aborda como segundo eje, **el desarrollo de nuevos perfiles de talento y nuevos programas y formatos de formación de competencias.** Finalmente, el tercer eje de trabajo está integrado por los **mecanismos de asociación público-privada** y centralización de instituciones para la formación de talento en distintos niveles. El detalle de las once iniciativas se puede ver a continuación.

Las iniciativas propuestas por este equipo de trabajo se agrupan bajo tres ejes. De ellas 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.	11 Asociación público-privada para generación de programas que desarrollen talentos.
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.	

COMITÉ DE DESARROLLO
CULTURA EN CIBERSEGURIDAD

El foco de trabajo de este segundo comité estuvo puesto en el desarrollo de mecanismos de adopción de buenas prácticas y ciberhigiene en ciberseguridad, permeando la cultura y el comportamiento organizacional. Esto aplica tanto a nivel de directorios como de colaboradores. Así mismo, se considera la cultura en ciberseguridad de usuarios y ciudadanía.

OBJETIVO

El objetivo de esta mesa de trabajo fue desarrollar el diseño y propuestas de implementación de un portafolio de iniciativas a nivel táctico, conteniendo proyectos de desarrollo privados, propuestas de política pública y/o de colaboración entre distintos sectores, enfocándose en las problemáticas asociadas al cierre de brechas de cultura en ciberseguridad local.

VISIÓN

Como línea base de discusión del Comité de Cultura, se definió una visión de futuro audaz que refleja la imagen del cambio y del éxito que se visualiza para el país en los próximos años y el impacto que se aspira generar con las iniciativas propuestas.

Visión audaz de futuro

"El/la ciudadano/a chileno/a del futuro será una persona que, sin importar género ni estatus socioeconómico, tendrá acceso a oportunidades para el desarrollo de una conciencia de riesgos digitales y un comportamiento efectivo, seguro y resiliente para la prevención y acción frente a ciberataques".

OBJETIVOS ESPECÍFICOS E INDICADORES DE DESEMPEÑO NOTABLES

Con el fin de enmarcar y orientar el trabajo e impacto de los proyectos propuestos, se delimitaron ocho objetivos de trabajo que describen el área de intervención declarada por este comité. Los objetivos están orientados a realizar definiciones de las competencias mínimas que componen una conciencia fundamental en temas de ciberseguridad, la definición de *benchmarks* de cultura a nivel nacional, y el desarrollo de instrumentos específicos de generación de competencias básicas, que habiliten cambios de comportamiento efectivos frente a las interacciones digitales, entre otros. Cada uno de estos objetivos tiene métricas e indicadores de éxito claros que permiten hacer un seguimiento concreto del impacto que el portafolio generará en el ecosistema. A continuación, se presentan las tablas resúmenes de ambos puntos.

OBJETIVOS	INDICADORES
1 Definir cuáles son los elementos de conciencia y comportamiento respecto a ciberseguridad y levantar una línea base de diagnóstico.	• # N Nivel de madurez en cultura de ciberseguridad nacional y desagregado por industrias. • Como línea base se sugiere la utilización de las mismas dimensiones de madurez aplicadas en el Global Cybersecurity Index de Oxford.
2 Generar un benchmark para analizar las brechas, y también pymes y startups, para desarrollar un ecosistema y llegar a la visión de que Chile es un país seguro para el desarrollo de empresas e inversiones.	• Como línea base se sugiere la utilización de las mismas dimensiones de madurez aplicadas en el Global Cybersecurity Index de Oxford.
3 Desarrollar competencias para la transferencia de conocimiento de principios básicos de seguridad digital.	• # N Puntaje de Nivel de conocimiento de ciberseguridad en la población. • % de gente que identifica las 5 capacidades clave en cultura de ciberseguridad. • % Adopción de contenidos de ciberseguridad en programas de educación básica, media y superior. • N empresas que incorporan directores con conocimientos en ciberseguridad
4 Configurar una institucionalidad que sea capaz de medir cuantitativa y cualitativamente el cambio de comportamiento.	• Hito de creación institucionalidad
5 Desarrollar mecanismos de certificación para pymes.	• % Implementación de programas de capacitación en empresas • % de pymes que han incorporado la ciberseguridad como pilar de desarrollo • % de empresas/ pymes que tienen programas de concientización en ciberseguridad. • N Puntaje Nivel de sensación de seguridad digital • Nivel de confianza en los canales digitales de organizaciones en el país (gobierno y otras)
6 Desarrollar mecanismos de certificación para pymes.	• Nivel de confianza en los canales digitales de organizaciones en el país (gobierno y otras)
7 Desarrollar capacidades de auditoría en la implementación de estándares de ciberseguridad.	•N número de auditores capacitados en estándares de ciberseguridad
8 Desarrollar capacidades de auditoría en la implementación de estándares de ciberseguridad.	•% adopción de mejores prácticas de ciberseguridad en empresas, por segmento (grandes/ pymes), como el uso de softwares que reducen los riesgos de ciberataques. •% adopción y uso de estándares de ciberseguridad en procesos de adquisición.

REFLEXIONES GENERALES DEL COMITÉ

Dentro de las reflexiones principales que surgieron de la conversación de esta mesa de trabajo, se planteó en primera instancia la idea de **diseñar un portafolio pensando siempre en centrar la visión en el perfil de ciudadano del futuro que se quiere formar para el Chile de 2035**. De esta manera, el diseño de las iniciativas privadas y de política pública deberían tener siempre en consideración las brechas actuales que existen para alcanzar el nivel de formación de ciudadano digital que necesita el país, de acuerdo a la senda de desarrollo y crecimiento sostenible que se espera a futuro. De esta manera, el elemento cultural es un habilitante transversal para la construcción de la confianza y resiliencia digital del Chile futuro.

Por otro lado, **se reflexiona sobre la relevancia de la conciencia de riesgos y cambio efectivo de comportamiento y desarrollo de competencias**. El cambio cultural no se sostiene únicamente en la transferencia de conocimiento general y técnico sobre ciberseguridad, sino que esta debe traducirse en conductas responsables, de prevención, reacción y mitigación adecuadas ante eventos de ciberseguridad.

Dentro de las brechas que se destacan surge la importancia de realizar una definición cualitativa de las dimensiones de intervención más importantes en temas temporales y complementarlo con levantamientos de mecanismos de levantamiento cuantitativo del nivel de madurez de cultura.

Finalmente, se reconoce como una dimensión de la complejidad del desafío que lo cultural se debe abordar a nivel transversal, tanto dentro de las organizaciones como a nivel ciudadano. Por lo tanto, **los espacios de intervención no son únicamente aquellos dentro de las instituciones o empresas privadas, sino también dentro del sector público y la ciudadanía de forma transversal.**

PROPUESTAS DE PROYECTOS

El portafolio de esta área se compone de **diecisiete iniciativas de cultura en ciberseguridad**, enfocadas principalmente en **cuatro ejes de trabajo.** Primero, como eje se proponen **iniciativas asociadas al desarrollo de hábitos y autocuidado ciudadano**, entendiendo que la población general, tanto en su rol de ciudadanos como de consumidores o clientes digitales, se ven altamente expuestos a los riesgos de ataques. Es por eso que el primer eje se enfoca en la concientización y en lograr un amplio alcance e impacto.

El segundo eje de trabajo engloba **iniciativas enfocadas en el desarrollo de cultura en organizaciones**, desde pymes hasta medianas y grandes empresas. Este eje apunta a la generación de reconocimiento de las buenas prácticas por medio de la visualización de casos de éxito por un lado, hasta la generación de evidencia del impacto de la ciberseguridad en el negocio y la construcción de espacios de confianza para compartir prácticas y experiencias en ciberseguridad entre distintos actores de las industrias. Este último punto es interesante, considerando que actualmente las redes del cibercrimen cuentan con sistemas sumamente sofisticados de colaboración, lo cual es aún un desafío por parte del ecosistema y la industria.

Como tercer eje, el foco de los proyectos está puesto en la **cultura en ciberseguridad dentro del Estado**, especialmente a propósito de la transformación digital estatal y, así mismo, el desafío de la territorialidad y descentralización de esfuerzos que permitan mayor alcance en la concientización de riesgos digitales.

Finalmente, una capa transversal propuesta como eje está asociado a las **capacidades de apoyo ante incidentes**. Este eje surge a propósito de las reflexiones del comité, en donde se identificó un espacio no resuelto respecto a las redes de apoyo en caso de incidentes, tanto para personas como organizaciones. Así como actualmente existen fonos de ayuda en el caso de delitos, o tomando como ejemplo que el Ministerio de Economía cuenta con sus plataformas como “Digitaliza tu pyme” o “Empresa en un día” y otros portales que centralizan información ante necesidades de transformación digital o formalización de empresas, **no existe con claridad un homólogo local para temáticas de ciberseguridad** más allá de los valiosos esfuerzos que se realiza al nivel del CSIRT. Es por esto que se propone un eje a cargo de esa orquestación y centralización de apoyo ante el ciberdelito. El resumen de las diecisiete iniciativas se puede ver a continuación.

PROPUESTAS DE PROYECTOS

Las iniciativas propuestas por este equipo de trabajo se agrupan bajo tres ejes. De ellas se priorizaron los proyectos 1, 12, 14 y 16.

DESARROLLO DE HÁBITOS Y AUTOCUIDADO CIUDADANOS

1. Ciclo de charlas en colegios que presenten ejemplos simples a los niños y niñas de cómo cuidarse en sus interacciones digitales.
2. Campaña comunicacional de concientización sobre riesgos digitales e importancia de hábitos de ciberseguridad.
3. Programa de concientización con la Bolsa de Santiago.
4. Campaña piloto Gobierno Digital.
5. Crear una campaña nacional de ciberseguridad.
6. Generar repositorio de material de libre uso.
7. Ciclo de charlas en colegios que presenten ejemplos simples a los niños y niñas de cómo cuidarse en sus interacciones digitales.

DESARROLLO DE CULTURA EN PYMES, EMPRESAS E INSTITUCIONES

8. Premio Nacional de Ciberseguridad para reconocer los comportamientos, conductas y hábitos que generen una cultura fuerte en el tema.
9. Generar herramientas básicas de auto evaluación para que las empresas, colegios y demás entidades puedan utilizar para conocer su nivel de madurez.
10. Fomentar y compartir a nivel institucional, público y privado, la experiencia de haber enfrentado eventos de ciberseguridad.
11. Generación de entornos de confianza. Ejemplos. Sandbox o procesos de anonimización. Información técnica.
12. Generar datos sobre el crecimiento / madurez en ciberseguridad a nivel nacional / o industrias claves (educación, salud, otros).
13. Impacto económico de los ataques. Foco Directorio.

DESARROLLO DE CULTURA A NIVEL DE TERRITORIO Y ESTADO

14. Difusión física / digital sobre elementos de ciberseguridad esenciales con foco local/regional a través de agencias locales (por ej. municipalidad).
15. Generar coordinaciones para apoyar a las organizaciones distribuidas en el país (CESFAM, hospitales, colegios, liceos, carabineros, otros).
16. Diseñar una serie de indicadores medibles que permitan a los auditores y otros conocer el nivel de avance en ciberseguridad y dar visibilidad periódica.

DESARROLLO DE CAPACIDADES DE APOYO ANTE INCIDENTES

17. Establecer canales de recepción de dudas y apoyo a las víctimas de ciberdelitos, por ejemplo, crear el CiberFono para atender dudas y emergencias.

COMITÉ DE DESARROLLO
TECNOLOGÍA, ECOSISTEMA, PROTOCOLOS Y ESTÁNDARES DE CIBERSEGURIDAD

El foco del tercer comité estuvo puesto en la implementación y desarrollo de tecnología habilitante para las estrategias de ciberseguridad y la mejora de procesos internos y de negocios. En esta línea se contempla tanto el uso de tecnología y la creación de ecosistemas tecnológicos, como la implementación de normas, protocolos y estándares que van de la mano de la implementación tecnológica.

OBJETIVO

El objetivo de esta mesa de trabajo fue desarrollar el diseño y propuestas de implementación de un portafolio de iniciativas a nivel táctico, conteniendo proyectos de desarrollo privados, propuestas de política pública y/o de colaboración entre distintos sectores, enfocándose en las problemáticas asociadas al cierre de brechas de tecnología, ecosistemas, protocolos y tecnologías para la ciberseguridad.

VISIÓN

Como línea base de discusión del Comité de Tecnologías, ecosistemas, protocolos y estándares, se definió una visión de futuro audaz que refleja la imagen del cambio y del éxito que se visualiza para el país en los próximos años y el impacto que se aspira generar con las iniciativas propuestas.

Visión audaz de futuro

"Chile es un país y un ecosistema regional tecnológico robusto en ciberseguridad que cuenta con sistemas formales de colaboración, desarrollo de cultura, espacios de experimentación tecnológica y protocolos de implementación de tecnología, estándares y normativas que sostienen procesos críticos del país públicos y privados, velando por la protección de datos y componiendo un sistema digital resiliente frente al combate de la ciberdelincuencia"

OBJETIVOS ESPECÍFICOS E INDICADORES DE DESEMPEÑO NOTABLES

Con el fin de enmarcar y orientar el trabajo e impacto de los proyectos propuestos, se definieron siete objetivos de trabajo que describen el área de intervención declarada por este comité. Los objetivos específicos están orientados, en primera instancia, a desarrollar levantamientos de estándares y normas que se puedan adaptar localmente, identificando los espacios de oportunidad de adopción temprana, preparándonos y adelantándonos a implementaciones de estándares regulados. Por otro lado, también se reconocen las capacidades técnicas en las áreas de auditoría en ciberseguridad, donde se encuentran grandes espacios de oportunidad actualmente. Así mismo, estos también apuntan al desarrollo de capacidades de monitoreo de estándares y espacios de experimentación tecnológica para la ciberseguridad, entre otros. Cada uno de estos objetivos tiene métricas e indicadores de éxito claros que permiten hacer un seguimiento concreto del impacto que el portafolio generará en el ecosistema. A continuación, se presentan las tablas resúmenes de ambos puntos.

OBJETIVOS	INDICADORES
1 Desarrollar un levantamiento de estándares tecnológicos necesarios en la industria y que aún no han sido adoptados.	• Niveles de inversión en ciberseguridad. • % Niveles de adopción de determinadas tecnologías relevantes por tamaño de empresa. • Número de startups o empresas con foco de negocios en ciberseguridad que se crean en Chile.
2 Desarrollar capacidades de auditoría técnica y certificaciones en ciberseguridad.	• Número de auditores capacitados en estándares de ciberseguridad.
3 Desarrollar capacidades de adaptación de estándares internacionales para la industria local .	• Hito: Levantamiento estándares de potencial implementación en Chile.
4 Desarrollar plataformas para el monitoreo de estándares y su adopción.	• Hito de creación o consolidación de plataformas de monitoreo. • Tasa de difusión y visualización de material técnico audiovisual que explique los conceptos básicos de ciberseguridad y sus estándares. • Tasa de difusión y visualización de material técnico audiovisual que explique los conceptos básicos de ciberseguridad y sus estándares.
5 Desarrollar mecanismos para incidir en los estándares y exigencias a los proveedores tecnológicos y de la cadena de valor de las empresas.	• % Niveles de adopción de determinadas tecnologías relevantes por tamaño de empresa. • Número de empresas que han adoptado el estándar determinado.
6 Facilitar el aumento en el nivel de madurez del ecosistema por medio de estándares de seguridad informática básica.	• Como línea base se sugiere la utilización de las mismas dimensiones de madurez aplicadas en el Global Cybersecurity Index de Oxford. • Número de empresas con una postura de ciberseguridad definida.
7 Desarrollar capacidades de experimentación y desarrollo de pruebas/ pilotajes de tecnologías para la ciberseguridad.	• Hito de creación o consolidación de plataformas de monitoreo. • Tasa de difusión y visualización de material técnico audiovisual que explique los conceptos básicos de ciberseguridad y sus estándares. • Tasa de difusión y visualización de material técnico audiovisual que explique los conceptos básicos de ciberseguridad y sus estándares.

REFLEXIONES GENERALES DEL COMITÉ

Una de las principales directrices de trabajo del comité estuvo en focalizarse en la **implementación y homologación de normas y estándares de ciberseguridad, adecuadas a las distintas industrias.** Este foco se sostiene sobre la base de que actualmente existen tecnologías y estándares internacionales relevantes que pueden adaptarse a la realidad local y facilitar su implementación pertinente.

Por otro lado, se plantea la necesidad de **incorporar la visión de la cadena de valor en su conjunto**, considerando que la ciberseguridad no está alojada únicamente dentro de los departamentos de TI o tecnología, sino que requiere esfuerzos de implementación transversales en la organización.

Finalmente, se reconoce y se destaca la **necesidad de que las tres áreas, tanto talento, como cultura y tecnología se aborden de forma integrada**, especialmente, incorporando dentro de la visión global elementos asociados al componente de personas. En esta línea, se reconoce la dimensión cultural y de personas que involucra la adopción tecnológica y desde esta perspectiva se plantean las iniciativas de trabajo.

PROPUESTAS DE PROYECTOS

El portafolio de esta área se compone de **catorce iniciativas de cultura en ciberseguridad**, enfocadas principalmente en **tres ejes de trabajo**. Primero, un eje de trabajo agrupa a aquellos proyectos que apuntan a la **difusión y adopción de normativas y estándares**. La idea de este primer bloque de proyectos está asociada a la generación de un catastro y definición de brechas de estándares, junto con material para la adopción e implementación de frameworks de ciberseguridad, de acuerdo al tamaño de cada empresa.

Como segundo eje, se plantea un bloque de proyectos que apuntan hacia el **desarrollo de herramientas tecnológicas para llevar a cabo la trazabilidad y monitoreo de las normativas y estándares adoptados.** Este punto es relevante para poder medir y cuantificar los niveles de madurez basales y los avances en materia de ciberseguridad en las industrias chilenas.

Finalmente, el tercer eje está asociado al **ecosistema y sus mecanismos de cooperación efectiva.** Principalmente, este eje apunta a modelos de colaboración e institucionalidad, como la creación de asociaciones que puedan apoyar a sectores como las pymes en materias de ciberseguridad. El resumen de las catorce iniciativas se puede ver a continuación.

PROPUESTAS DE PROYECTOS

Fruto del trabajo de esos Comités de Desarrollo se presentaron doce propuestas de proyectos, de las cuales el Comité Asesor priorizó cuatro. Esas iniciativas se detallan en el portafolio de esta Hoja de Ruta. Las ocho restantes se presentan en el Anexo.

DIFUSIÓN Y ADOPCIÓN DE NORMATIVAS Y ESTÁNDARES

1. Catastro de estándares: 1. Qué es lo que hay. 2. Qué es lo que tenemos, 3. Cuáles son los que conviene adoptar.
2. Documentos "Consejos de ciberseguridad": apoyo a la implementación de ciberseguridad.
3. Material práctico para la implementación de los estándares y frameworks escogidos, segmentado.
4. Kit Digital" para pymes sobre ciberseguridad.
5. Protección de Datos. Generación de documentación y material práctico de implementación técnica y de cara del consumidor y del negocio.
6. "¿Cómo cuidar tu nube?" Difusión de prácticas básicas en diversas nubes (Azure/AWS/Google/ etc.).
7. Implementar el estándar de Identidad Digital, homologando el caso de Estonia.
8. Generar un protocolo de actuación ante un ciberataque. Qué es lo que tengo que hacer si soy víctima, como empresa, de un ciberataque.

MONITOREO DE CUMPLIMIENTO Y MÉTRICAS

9. Herramientas o plataformas de autoevaluación para definir el estado actual de las empresas respecto de un estándar.
10. Plataforma Cloud de monitoreo y cumplimiento de normas, tomando como primer MVP piloto el caso del NERC CIP para 700 empresas del sistema eléctrico nacional.

COOPERACIÓN Y ECOSISTEMA

11. Crear una entidad que promueva la ciberseguridad a nivel de pymes, aprovechando las redes de las asociaciones gremiales.
12. Generar un fondo de promoción de ciberhigiene.
13. Creación de una organización nueva o ampliar capacidades de INN en Chile para facilitar adopción de estándares
14. Implementar la obligatoriedad de cierto nivel demostrable de ciberseguridad, a nivel del estado
15. Mecanismos de comunicación y transparencia en los eventos y vulnerabilidades.

0.6 PORTAFOLIO

PORTAFOLIO

Como resultado final de la metodología aplicada en esta Hoja de Ruta, se analizaron las 42 ideas de proyectos y priorizaron en cada Comité de Desarrollo aquellos con mayor potencial de alcance e impacto. De este proceso, los tres comités lograron consolidar un portafolio de doce proyectos con un horizonte de trabajo de tres años. A continuación, se muestra el resumen del portafolio final.

TALENTO Y DESARROLLO DE COMPETENCIAS PARA LA CIBERSEGURIDAD	CULTURA EN CIBERSEGURIDAD	TECNOLOGÍA, ESTÁNDARES, PROTOCOLOS Y ECOSISTEMAS PARA LA CIBERSEGURIDAD
A.1 PILOTAJE DE PROGRAMA DE MAGÍSTER EN CIBERSEGURIDAD BID	B.1 CAMPAÑA COMUNICACIONAL DE CONCIENTIZACIÓN SOBRE RIESGOS DIGITALES E IMPORTANCIA DE HÁBITOS DE CIBERSEGURIDAD B.1.1 Programa de concientización con la Bolsa de Santiago B.1.2 Repositorio de material de libre uso	C.1 ESTUDIO DE LEVANTAMIENTO DE ESTÁNDARES Y BRECHAS DE ADOPCIÓN: · Qué es lo que hay · Qué es lo que tenemos · Cuáles son los que conviene adoptar
A.2 PROGRAMAS DE EDUCACIÓN CONTINUA PARA FORMACIÓN EN CIBERSEGURIDAD	B.2 FOMENTO A NIVEL INSTITUCIONAL PÚBLICO Y PRIVADO DEL TRASPASO DE EXPERIENCIAS DE ENFRENTAMIENTO DE EVENTOS DE CIBERSEGURIDAD B.2.1 Generación de Entornos de Confianza: Sandbox o procesos de anonimización	C.2 APOYO A LA IMPLEMENTACIÓN DE CIBERSEGURIDAD A TRAVÉS DEL DOCUMENTO "CONSEJOS DE CIBERSEGURIDAD" C.2.1 Material práctico y segmentado para la implementación de los estándares y frameworks escogidos C.2.2 "Kit Digital" para pymes sobre ciberseguridad
A.3 DISPONIBILIDAD DE CENTROS DE DESARROLLO DE TALENTOS A NIVEL ESCOLAR: PILOTO PROGRAMA DE ESCUELAS ABIERTAS	B.3 GENERACIÓN DE DATOS SOBRE EL CRECIMIENTO/ MADUREZ EN CIBERSEGURIDAD A NIVEL NACIONAL O INDUSTRIAS CLAVES (EDUCACIÓN, SALUD, OTROS). IMPACTO ECONÓMICO DE LOS ATAQUES	C.3 BUENAS PRÁCTICAS DE USO DE LA NUBE Difusión de prácticas básicas en diversas nubes (Azure, AWS, Google, etc.)
A.4 ASOCIACIÓN PÚBLICO-PRIVADA PARA LA GENERACIÓN DE PROGRAMAS QUE DESARROLLEN TALENTOS	B.4 CANALES DE RECEPCIÓN DE DUDAS Y APOYO A LAS VÍCTIMAS DE CIBERDELITOS. POR EJEMPLO: CREAR UN CIBERFONO O PORTAL DE AYUDA	C.4 PLATAFORMA DE MONITOREO DE NORMAS. Herramientas o plataformas de autoevaluación para definir el estado actual de las empresas respecto de un estándar

De estos doce proyectos propuestos por los tres Comités de Desarrollo, cuatro fueron priorizados por el Comité Asesor. A continuación se detallan los paquetes de proyectos priorizados.

PAQUETE DE TRABAJO PRIORIZADO 1 (A2)

En la dimensión de talento, uno de los puntos priorizados es el desarrollo de programas de educación continua para implementar en empresas con necesidades de capacitación. Esta iniciativa apunta hacia los requerimientos de actualización de capacitación y especialización, renovando las habilidades y contenidos aprendidos por los colaboradores de las organizaciones.

La visión está asociada a alinearse con el cumplimiento de la meta de 10.000 profesionales nuevos especializados en ciberseguridad a nivel nacional para el 2035, de acuerdo a lo establecido en la Estrategia Nacional de Transformación Digital. A continuación, se presenta la ficha técnica resumida del proyecto propuesto.

A.2 PROGRAMAS DE EDUCACIÓN CONTINUA PARA FORMACIÓN EN CIBERSEGURIDAD

OBJETIVO

Aumentar la oferta académica de educación continua para el desarrollo de especializaciones en ciberseguridad.

IDEA

Difundir e implementar el Programa in-company con foco interdisciplinario.

VISIÓN 2035

Alcanzar al menos 20.000 profesionales nuevos especializados en ciberseguridad.

FRICCIONES O RIESGOS

- Riesgos culturales y adaptaciones por industrias necesarias para que los programas de capacitación en ciberseguridad sean efectivos.

SEGMENTO OBJETIVO

- Empresas con áreas de ciberseguridad
- Equipos que manejan, gestionan o implementan, a nivel técnico o como soporte, actividades relacionadas a la ciberseguridad.

IMPACTO ESPERADO A TRES AÑOS:

- Contar con al menos 150 empresas participando en los programas.

PROYECTO MÍNIMO VIABLE (PMV)

- Programa de educación continua con foco interdisciplinario.
- Los programas de educación continua son modulares y permiten customizar las temáticas y el nivel de profundidad en ciberseguridad de acuerdo a los perfiles de los participantes y rubro de la empresa.

PAQUETE DE TRABAJO PRIORIZADO 2 (A4)

Uno de los principales puntos priorizados por el Comité Asesor de la Hoja de Ruta es la relevancia de crear mecanismos para la generación de programas de formación flexibles y ágiles, que se hagan cargo de las brechas de talento en ciberseguridad. Uno de los componentes fundamentales es que este tipo de programas contemplen la colaboración del sector industrial, capturando de forma efectiva la demanda real de competencias técnicas y transversales asociadas a la ciberseguridad.

Para alcanzar esta visión, la idea propuesta es empujar hacia el desarrollo de asociaciones público-privadas, bajo las cuales se generen programas de desarrollo de talento, con foco en segmento técnicos y profesionales jóvenes en industrias donde la ciberseguridad es clave. Este proyecto, en el largo plazo, busca alinearse con la eventual creación del Instituto Nacional de Ciberseguridad, propuesto en la Ley Marco, que se encuentra aún en discusión a diciembre de 2022. A continuación, se presenta la ficha técnica resumida del proyecto propuesto.

A.4 ASOCIACIÓN PÚBLICO-PRIVADA PARA LA GENERACIÓN DE PROGRAMAS QUE DESARROLLEN TALENTOS

OBJETIVO

Facilitar la formación de habilidades digitales en ciberseguridad.

IDEA

Asociación o consorcio entre empresa(s) de la industria tecnológica con el Ministerio de Educación y alguna institución de educación para crear planes de formación que logren desarrollar los talentos requeridos (piloto escalable).

VISIÓN 2035

Creación del Instituto Nacional de Ciberseguridad (participación y financiamiento público-privada)

FRICCIONES O RIESGOS

- Falta de talentos en el mercado para los próximos cinco años.
- Falta de desarrollo orgánico en la formación de especialistas (10.000 talentos al 2035).

SEGMENTO OBJETIVO

- Técnicos y profesionales jóvenes interesados en temas de ciberseguridad, con especial foco en profesionales con perfiles para empresas de tipo Telecomunicaciones, Financieras, etc., que cubran un amplio rango de tipos de servicios y/o industrias.

IMPACTO ESPERADO A TRES AÑOS:

- Contar con al menos 150 empresas participando en los programas.

PROYECTO MÍNIMO VIABLE (PMV)

- Desarrollo de un Programa piloto de formación público-privada-academia.
- Alcance inicial: 500 personas
- 6 meses.

PAQUETE DE TRABAJO PRIORIZADO 3 (B1)

Uno de los elementos fundamentales dentro de la discusión de la ciberseguridad, es la generación de cambios conductuales efectivos. La exposición exponencial a los medios digitales a través de las compras, la formación y los trámites en línea, junto con la navegación en redes sociales, entre otros, ha gatillado una amplificación de segmentos de la población que se ven expuestos constantemente a potenciales ataques cibernéticos. En esta línea, es crítica la necesidad de concientización de forma generalizada y con el mayor alcance ciudadano posible, para generar un impacto en la disminución de delitos cibernéticos prevenibles por vías de la ciberhigiene.

Es en esta línea que se propone poner foco en esfuerzos que apoyen el desarrollo de campañas comunicacionales de concientización de los riesgos digitales y la relevancia de los hábitos de la ciberseguridad. Si bien, actualmente existen iniciativas del sector público, como las campañas desarrolladas por el CSIRT junto a asociaciones y sectores del retail y la banca, existe aún un espacio para potenciar el mensaje y escalar los esfuerzos de forma transversal y constante a la ciudadanía. A continuación, se presenta la ficha técnica resumida del proyecto propuesto.

B.1 CAMPAÑA COMUNICACIONAL DE CONCIENTIZACIÓN SOBRE RIESGOS DIGITALES E IMPORTANCIA DE HÁBITOS DE CIBERSEGURIDAD

OBJETIVO

Desarrollar concientización sobre riesgos digitales e importancia de hábitos de ciberseguridad.

IDEA

Programa de concientización con la Bolsa de Santiago u otro segmento de comercios.

VISIÓN 2035

- Cada página del sector público o privado, mostrará un aviso sobre la importancia de la ciberseguridad, con listado de acciones para resguardar seguridad digital y un enlace al sitio de mitigación o ayuda en caso de ser víctima digital.
- Que toda sociedad anónima abierta cuente con un sistema de gestión de riesgo asociado a la seguridad de la información.

FRICCIONES O RIESGOS

- Desconocimiento de los riesgos y medidas para gestionarlos y aminorarlos.
- Ausencia de conocimiento y gestión de riesgos asociados a seguridad de la información.

SEGMENTO OBJETIVO

- Ciudadanía
- Empresas con canales digitales de venta.

IMPACTO ESPERADO A TRES AÑOS:

- Implementación de al menos dos campañas de difusión al año.
- Repositorio de material audiovisual y técnico de uso abierto para empresas e instituciones.

PROYECTO MÍNIMO VIABLE (PMV)

- Implementación de programas de prevención en el segmento objetivo.
- Plan comunicacional segmentado por mercado/industrias.
- Generación de material gráfico y audiovisual a disposición de los sectores retail, banca y pymes para integrar en sus sitios web.

PAQUETE DE TRABAJO PRIORIZADO 4 (C4)

Finalmente, dentro de las líneas críticas de trabajo está la disponibilización de herramientas que permitan el monitoreo y trazabilidad del cumplimiento de normas en ciberseguridad. Una de las principales preocupaciones que habilitan esta iniciativa es el nivel de adopción de normas y estándares de ciberseguridad por parte de los distintos sectores industriales a nivel país.

La adopción de normativas habilita la creación de cambios en protocolos, implementación tecnológica adecuada y cambios en comportamientos relevantes que son monitoreados y reportados por parte de las empresas. La adopción de normativas y, posteriormente, de estándares de ciberseguridad, presenta un espacio importante de oportunidad, tanto en la etapa de evaluación del nivel de madurez actual de una compañía, como la reportería y medición del nivel de avance en la adopción efectiva de las normativas elegidas. Este espacio de oportunidad también se abre hacia la potencial homologación de la reportería y auditoría en cumplimiento de normativas y como potencial herramienta para los entes reguladores de las distintas industrias. El sector eléctrico es uno de los ejemplos en donde se podrían iniciar los primeros proyectos mínimos viables, con potencial de escalamiento a otras áreas. A continuación, se presenta la ficha técnica resumida del proyecto propuesto.

C.4 PLATAFORMA DE MONITOREO DE NORMAS

OBJETIVO
Generar plataformas para evaluación del cumplimiento de normas y/o estándares industriales.

IDEA
Plataforma Cloud de monitoreo y cumplimiento de normas.
- Etapa 1: Desarrollo de assessment digital.
- Etapa 2: Cumplimiento y monitoreo normativo PMV piloto NERC CIP para 700 empresas del sistema eléctrico nacional.

VISIÓN 2035
Plataforma de monitoreo de normas disponibles para todas las industrias de forma transversal.

REFERENTES
NERC de EE.UU. También existe una relación directa con operadores independientes como el IESO de Canadá.

FRICCIONES O RIESGOS
- Avanzar en forma consistente y sustentable con información y nivel de avance en cumplimiento de normativas estandarizadas.

SEGMENTO OBJETIVO
- Empresas sujetas a potenciales cumplimientos normativos y estándares.
- Para el PMV se propone enfocar el proyecto en el sector eléctrico y las empresas sujetas a regulación del CEN.

IMPACTO ESPERADO A TRES AÑOS:
- Inicialmente, aproximadamente 700 empresas, con un alto impacto por tratarse de un sector de infraestructura crítica y que soporta servicios esenciales como Salud, Transporte, Telecomunicaciones, Minería, entre otros.

PROYECTO MÍNIMO VIABLE (PMV)
- Al ser transversal al sector eléctrico (generadoras, transmisoras, distribuidoras y clientes libres) el objetivo es lograr una plataforma que facilite, proteja y reporte los niveles de cumplimiento del estándar, generando vistas de niveles de riesgo y mapas de calor interesantes a la hora de definir nuevas estrategias de protección y defensa sectorial.

0.7 CONCLUSIONES Y PERSPECTIVAS FUTURAS

CONCLUSIONES Y PERSPECTIVAS FUTURAS

El desarrollo de esta Hoja de Ruta ha significado un proceso de creación colaborativa y sinérgica en el que han participado alrededor de cien actores del sector público, privado, civil y de la academia. Este esfuerzo multisectorial da cuenta de la relevancia estratégica y transversal que supone la ciberseguridad en nuestro ecosistema. **Al inicio de este proceso, la ciberseguridad ya era un tema crítico para habilitar la adopción tecnológica y la transformación digital del país y, sobre todo, del sector pymes**. Este punto toma aún más relevancia desde la perspectiva de la información y su infraestructura asociada, como activos estratégicos para la toma de decisiones, tanto a nivel público como privado.

Una de las líneas base del trabajo desarrollado fue la definición común de ciberseguridad más allá de la dimensión técnica estereotipada que tiende a asociarse a las áreas de IT o Tecnologías de la Información. **Uno de los principales aportes de este trabajo es la visión holística integrada con la que se aborda la ciberseguridad, caracterizada como un proceso sistemático descrito en el modelo multidimensional propuesto**. Bajo esta perspectiva, así como existen variables internas dentro de las organizaciones con dimensiones de negocios, talento, protocolos y tecnologías, también se hallan dimensiones ecosistémicas relevantes. Por ejemplo, desde el punto vista legal-regulatorio, el proyecto de ley marco de ciberseguridad toma especial relevancia para la conformación de una gobernanza e institucionalidad nacional en la materia. De esta misma manera, se contemplan en la discusión elementos fundamentales como las infraestructuras críticas habilitantes, los incentivos de inversión, los mecanismos de creación de industrias, la generación de conocimiento por medio de investigación avanzada, y el desarrollo de emprendimientos de base científico-tecnológica, entre otros.

Sin duda, las **tres principales dimensiones priorizadas** en el desarrollo de los portafolios de trabajo presentan desafíos fundamentales que deben comenzar a abordarse de forma urgente. **En el área de talento, uno de los principales desafíos es el desarrollo de competencias por medio de programas flexibles y ágiles que permitan responder a las amenazas que se sofistican de forma exponencial**. Esto se manifiesta no sólo a nivel de formación profesional, sino también por medio de la formación escolar y técnica. La principal propuesta en esta línea es **generar e implementar modelos de formación conjunto entre los distintos actores del ecosistema y que permitan dinamizar y diversificar los espacios de desarrollo de competencias necesarias a nivel local**. Por otro lado, **en relación a la dimensión cultural, la ciberseguridad requiere cambios de conducta efectivos y concretos en todos los usuarios digitales**. Las conductas, de esta manera, no son únicamente aquellas expresadas en el contexto laboral, sino también las que están presentes en los contextos digitales personales y ciudadanos, que permean todo el manejo de la vida digital de las personas. En esta línea, **se propone el desarrollo de estrategias y campañas comunicacionales que permitan un alcance a escala nacional, relevante y significativo**. Aquí, nuevamente se requiere revisar la conducta y la alineación de la estrategia y visión de negocios con la identidad y comportamiento digital de las instituciones.

Finalmente, **la tercera dimensión asociada a tecnología, presenta reflexiones muy relevantes en la arista de incorporación y adopción efectiva de estándares y normas de ciberseguridad**. En esta línea, un espacio de oportunidad fundamental es la adopción de estándares industriales que permitan homologar el nivel internacional de cumplimiento y transitar de forma ágil hacia las normas y regulaciones mandatarias que se han empezado a implementar en distintas industrias. Es así como una de las propuestas clave es el desarrollo de plataformas que permitan hacer un seguimiento sistemático de la adopción de normas y estándares para los reguladores y las organizaciones. Cada una de estas tres dimensiones está permeada por

los desafíos transversales de inclusión, territorialidad y brechas de género ya existentes en el área STEM y aún más en el ambiente de la ciberseguridad, lo cual suma una capa de reflexión y de complejidad que acentúa la necesidad de colaboración conjunta.

El espíritu de este trabajo se ha enfocado en la dimensión táctica, es decir, en propuestas de implementación inmediata durante los próximos tres años. Esto dotará al portafolio de la velocidad y el momentum necesarios para escalar hacia iniciativas transformacionales, que logren habilitar el avance sistemático de Chile hacia mayores niveles de madurez en ciberseguridad, con el potencial de convertirse en un referente regional en esta materia.

De cara a las perspectivas futuras de esta Hoja de Ruta, el desarrollo de estructuras de trabajo asociativas entre actores de diversos sectores es clave para avanzar en el diseño de mecanismos de prevención, reacción y mitigación de incidentes en ciberseguridad, que sean ágiles y maduros. De esta manera, será posible enfrentar el avance vertiginoso del cibercrimen por medio de la institucionalidad, el talento, la tecnología y las mejores prácticas. **La invitación a todos los actores del ecosistema es a sumar esfuerzos y generar sinergias por medio de la complementariedad de las iniciativas, recursos y capacidades de cada organización y ciudadano**. Es tarea de todos aportar en la actualización constante de espacios de oportunidad para robustecer la competitividad local a través del fortalecimiento de la confianza y resiliencia digital.

0.8 ANEXO

Estos son los títulos de los ocho proyectos del portafolio no priorizados por el Comité Asesor.

COMITÉ DE TALENTO Y DESARROLLO DE COMPETENCIAS EN CIBERSEGURIDAD

- **A.1** PILOTAJE DE PROGRAMA DE MAGÍSTER EN CIBERSEGURIDAD BID
- **A.3** DISPONIBILIDAD DE CENTROS DE DESARROLLO DE TALENTOS A NIVEL ESCOLAR: PILOTO PROGRAMA DE ESCUELAS ABIERTAS

COMITÉ DE DESARROLLO DE CULTURA EN CIBERSEGURIDAD

- **B.2** FOMENTO A NIVEL INSTITUCIONAL PÚBLICO Y PRIVADO DEL TRASPASO DE EXPERIENCIAS DE ENFRENTAMIENTO DE EVENTOS DE CIBERSEGURIDAD
- **B.3** GENERACIÓN DE DATOS SOBRE EL CRECIMIENTO/MADUREZ EN CIBERSEGURIDAD A NIVEL NACIONAL O INDUSTRIAS CLAVES
- **B.4** CANALES DE RECEPCIÓN DE DUDAS Y APOYO A LAS VÍCTIMAS DE CIBERDELITOS

COMITÉ DE DESARROLLO DE TECNOLOGÍA, ESTÁNDARES, PROTOCOLOS Y ECOSISTEMAS DE CIBERSEGURIDAD

- **C.1** ESTUDIO DE LEVANTAMIENTO DE ESTÁNDARES Y BRECHAS DE ADOPCIÓN
- **C.2** APOYO A LA IMPLEMENTACIÓN DE CIBERSEGURIDAD A TRAVÉS DEL DOCUMENTO "CONSEJOS DE CIBERSEGURIDAD"
- **C.3** BUENAS PRÁCTICAS DE USO DE LA NUBE

A continuación se presentan fichas que resumen cada uno de los proyectos no priorizados.

A.1 PILOTAJE DE PROGRAMA DE MAGÍSTER EN CIBERSEGURIDAD BID

OBJETIVO

Aumentar la oferta académica profesional de postgrado para el desarrollo de especializaciones en ciberseguridad.

IDEA

Difundir e implementar el Programa de Magíster en Ciberseguridad de acuerdo a recomendaciones del BID.

VISIÓN 2035

Alcanzar al menos 5.000 profesionales nuevos especializados en ciberseguridad.

FRICCIONES O RIESGOS

- Largos tiempos de diseño y aprobación de los proyectos de creación de los programas de postgrado en IES.
- Adaptación de programas internacionales a los perfiles necesarios para las brechas de ciberseguridad del país.

SEGMENTO OBJETIVO

- Profesionales con título profesional en áreas de tecnología y afines cuyo rol esté vinculado a la gestión de la ciberseguridad.
- IES que adopten la creación de este tipo de magíster.

IMPACTO ESPERADO A TRES AÑOS:

- Contar con al menos una IES presencial y una IES Online implementando el magíster.
- Primera generación de sesenta participantes en una institución de educación superior.

PROYECTO MÍNIMO VIABLE (PMV)

- Adaptación local de la propuesta del Magíster en Ciberseguridad desarrollado como parte de las recomendaciones del BID.
- Implementación del programa en al menos 1 IES (Institución de Educación Superior)
- Inicio del proceso de acreditación del programa.

A.3 DISPONIBILIDAD DE CENTROS DE DESARROLLO DE TALENTOS A NIVEL ESCOLAR: PILOTO PROGRAMA DE ESCUELAS ABIERTAS

OBJETIVO

Generar centros para el desarrollo de talentos a nivel escolar que cuenten con herramientas y recursos.

IDEA

Piloto Escuelas Abiertas a través de la creación de programas de formación escolares coordinados por instituciones de educación superior.

VISIÓN 2035

Programa nacional Escuelas Abiertas Digitales. Referentes Estonia y sus programas de ciberseguridad en escuelas.

FRICCIONES O RIESGOS

- Baja prioridad en el currículo del Ministerio de Educación y colegios.
- Poca flexibilidad para cambiar el currículo del Ministerio de Educación.

SEGMENTO OBJETIVO

- Colegios técnicos y colegios particulares y subvencionados. Alumnos de colegios y escuelas que reciben financiamiento estatal y que postulen a los fondos del MINEDUC. (Principalmente colegios con baja calificación de desempeño)

IMPACTO ESPERADO A TRES AÑOS:

- El año 2019 el programa Escuelas Abiertas llegó a cerca de 68 mil estudiantes, se puede utilizar el mismo referente.

PROYECTO MÍNIMO VIABLE (PMV)

- Integrar a los programas del Ministerio de Educación "Escuelas Abiertas" y/o "Escuelas de Verano" con cursos y dinámicas que permitan desarrollar herramientas digitales.
- Abrir espacios fuera de los horarios de clases (fines de semana, vacaciones, etc.) para que estudiantes puedan aprender herramientas digitales de manera lúdica y segura.
- Se estima al menos poder llegar a diez escuelas en la primera etapa.

B.2 FOMENTO A NIVEL INSTITUCIONAL PÚBLICO Y PRIVADO DEL TRASPASO DE EXPERIENCIAS DE ENFRENTAMIENTO DE EVENTOS DE CIBERSEGURIDAD

OBJETIVO

Fomentar a nivel institucional público y privado, el traspaso de experiencias de haber enfrentado eventos de ciberseguridad.

IDEA

Un lugar donde las empresas/ instituciones, tanto públicas como privadas, ingresen y puedan consultar los incidentes de ciberseguridad, generando un área de colaboración para minimizar el crecimiento de los ataques.

VISIÓN 2035

Foro nacional de ciberseguridad. Tener una Base de Datos Nacional de Incidentes de Ciberseguridad.

FRICCIONES O RIESGOS

- Propagación de un ataque a otras empresas o instituciones.
- Falta de mecanismos de colaboración y mecanismos para la transferencia de conocimiento cruzado entre organizaciones víctimas de ciberataques.

SEGMENTO OBJETIVO

- Nivel nacional, para todas las organizaciones del Estado y privadas (pymes y grandes empresas).

IMPACTO ESPERADO A TRES AÑOS:

- Disminución de los impactos económicos que puede generar un ataque.
- Red de colaboración con instancias seguras de difusión de mejores prácticas y experiencias.

PROYECTO MÍNIMO VIABLE (PMV)

- Evento de difusión de experiencias y buenas prácticas.
- Storytelling. Canal de Youtube con "historias de guerra".
- Referente: TED Talks.

B.3 GENERACIÓN DE DATOS SOBRE EL CRECIMIENTO/MADUREZ EN CIBERSEGURIDAD A NIVEL NACIONAL O INDUSTRIAS CLAVES

OBJETIVO

Generar datos sobre el crecimiento y madurez en ciberseguridad a nivel nacional o en industrias claves (educación, salud, otros).

IDEA

- Desarrollar mediciones periódicas de indicadores de madurez digital por segmento e industria.
- Generar datos sobre madurez y entregar data para efectos de decisión de ciertos actores en mercados específicos.

VISIÓN 2035

Medición de eje de madurez cyber y cultura de forma periódica.

FRICCIONES O RIESGOS

- Necesidad de concientización en base a evidencia sobre los riesgos de ciberseguridad y su impacto en el negocio para los tomadores de decisiones.
- Necesidad de monitoreo estándar y trazable de la evolución de las vulnerabilidades digitales del país.

SEGMENTO OBJETIVO

- Nivel nacional, para todas las organizaciones del Estado y privadas (pymes y grandes empresas).

IMPACTO ESPERADO A TRES AÑOS:

- Disminución de los impactos económicos que puede generar un ataque.

PROYECTO MÍNIMO VIABLE (PMV)

- Medición trimestral / anual de indicadores estándar acerca de la actividad cibernética en Chile: considerando métricas como por ejemplo # incidentes, pérdidas, empresas afectadas, brecha de profesionales/profesionales que se gradúan en ciberseguridad.

B.4 CANALES DE RECEPCIÓN DE DUDAS Y APOYO A LAS VÍCTIMAS DE CIBERDELITOS

OBJETIVO
Generar plataforma de apoyo a la prevención de ciberataques.

IDEA
Establecer canales de recepción de dudas y apoyo a las víctimas de ciberdelitos, por ejemplo, crear el CiberFono para atender dudas y emergencias.

VISIÓN 2035
Asistente virtual automatizado.

FRICCIONES O RIESGOS
- La inexistencia de un conducto regular centralizado abierto para apoyo a las víctimas de ciberdelitos, con acceso a recursos y asesoría frente a un ciberataque, tanto a nivel de empresa como de ciudadanía.

SEGMENTO OBJETIVO
- Personas naturales que hagan uso de canales digitales.
- Empresas, especialmente pymes que cuenten con canales digitales y sistemas de información susceptibles a ataques cibernéticos.

IMPACTO ESPERADO A TRES AÑOS:
- Información centralizada y disponible en canal de atención digital y telefónico, abierto a todo público frente a consultas ante ciberataques.

PROYECTO MÍNIMO VIABLE (PMV)
- Generar un glosario de términos en ciberseguridad.
- Elaborar una guía rápida acerca de "¿Qué hacer si soy víctima de un ciberataque?".
- Generar un asistente virtual simple que guíe y transfiera a los usuarios a diversos insumos que permitan tomar acciones frente a distintas situaciones que enfrenten. Complementar con otros formatos para personas mayores.

C.1 ESTUDIO DE LEVANTAMIENTO DE ESTÁNDARES Y BRECHAS DE ADOPCIÓN

OBJETIVO
Entender qué han hecho países que han avanzado más que Chile en Ciberseguridad, y qué es lo que queremos emular.

IDEA
Catastro de estándares:
1. Qué es lo que hay.
2. Qué es lo que tenemos.
3. Cuáles son los que conviene adoptar.

VISIÓN 2035
Adopción de estándares.

FRICCIONES O RIESGOS
- Implementación y coordinación a nivel de industrias sobre brechas de desarrollo y adopción nacional de estándares.

SEGMENTO OBJETIVO
- Industrial, organismos reguladores, asociaciones gremiales.

IMPACTO ESPERADO A TRES AÑOS:
- Mayor facilidad en la adopción de estrategias de prevención.

PROYECTO MÍNIMO VIABLE (PMV)
- Desarrollo estudio de levantamiento y catastro de al menos tres industrias críticas a nivel nacional.

C.2 APOYO A LA IMPLEMENTACIÓN DE CIBERSEGURIDAD A TRAVÉS DEL DOCUMENTO "CONSEJOS DE CIBERSEGURIDAD"

OBJETIVO

Entrega de directrices, recomendaciones sobre qué implementar como medidas de ciberseguridad para la prevención y reacción de ciberataques.

IDEA

Documentos "Consejos de ciberseguridad": apoyo a la implementación de ciberseguridad

VISIÓN 2035

Recursos abiertos de apoyo que permitan la adopción de estándares internacionales homologados a la realidad local en al menos las 5 industrias más importantes de Chile.

FRICCIONES O RIESGOS

- Existen brechas importantes que generan fricciones de implementación de acciones para la ciberseguridad asociados a la disponibilidad y búsqueda de información, homologación de estándares y capacidades de implementación técnica.

SEGMENTO OBJETIVO

- Industria y organismos públicos a nivel general.

IMPACTO ESPERADO A TRES AÑOS:

- Al menos un estudio anual de levantamiento, catastro y recomendaciones de estrategias de adopción de estándares de ciberseguridad en tres industrias críticas chilenas.

PROYECTO MÍNIMO VIABLE (PMV)

- Seleccionar un estándar básico transversal a difundir.
- Material práctico para la implementación de los estándares y frameworks escogidos, segmentado.
- "Kit Digital" para pymes sobre ciberseguridad.

C.3 BUENAS PRÁCTICAS DE USO DE LA NUBE

OBJETIVO

Facilitar el conocimiento y toma de conciencia sobre mejores prácticas para el cuidado de la nube.

IDEA

"¿Cómo cuidar tu nube?" Difusión de prácticas básicas en diversas nubes (Azure / AWS / Google / etc.)

VISIÓN 2035

Repositorio transversal integrando distintos proveedores de nubes.

FRICCIONES O RIESGOS

- Ataques y pérdidas de información en despliegues realizados en nubes públicas o de manera híbrida.

SEGMENTO OBJETIVO

- Empresas medianas y grandes.

IMPACTO ESPERADO A TRES AÑOS:

- Plataforma integrada de información para la difusión de buenas prácticas.

PROYECTO MÍNIMO VIABLE (PMV)

- Consolidación de mejores prácticas para despliegues en la nube o despliegues híbridos para las principales nubes. Se puede hacer una consolidación de cinco o diez mejores prácticas que permitan limitar la capacidad de los atacantes. El foco debería estar en higiene (gobierno, administración), redes, protección de la información y protección de identidades.

0.9 REFERENCIAS Y BIBLIOGRAFÍA

REFERENCIAS Y BIBLIOGRAFÍA

Acronis. (2021). 10 crucial steps for protecting your company from cyber attacks. Acronis.

Aguiar, A. R. (2022, 31 de marzo). Así entregaron Facebook y Apple datos de usuarios a ciberdelincuentes. Business Insider España.

Australian Government. (2021, diciembre 21). Protect your business from cyber threats. Business.Gov.Au.

(BID) Ariel Nowersztern Santiago Paz Darío Kagelmacher Florencia Cabral Berenfus Pablo Libedinsky Computer Security Lab (COSEC) Arturo Ribagorda Juan Tapiador José María de Fuentes Lorena González. (2020). Programa formativo en ciberseguridad para América Latina y el Caribe.

Casas, L. (2018, 9 de junio) Robaron US$10 millones en ataque informático al Banco de Chile: virus fue un distractor. Bío-Bío Chile.

Brand Essence Research. (2021, noviembre). Cybersecurity Market Size, Industry Demand, Growth, Share & Forecast 2027. Brand Essence® Market Research and Consulting.

Canalys. (2020a, 9 de junio). Seven vendors crowned “Champion” in 2020 Cybersecurity Leadership . Canalys Newsroom.

Canalys. (2020b, 23 de junio). Cybersecurity Market Q1 2020. Canalys Newsroom.

Canalys. (2021, 7 de julio). Nine Vendors Ranked as Channel “Champions” in 2021 Cybersecurity Leadership Matrix. Canalys Newsroom.

Cisco. (2022). What is cybersecurity? Cisco.

CORFO. (2022). Ciberseguridad • Pymes en línea. Pymes En Línea.

CSIRT. (2021, 12 de junio). Gobierno y sector privado reafirman compromiso con la ciberseguridad con un convenio de colaboración. CSIRT.

CSIRT. (2022). Quiénes somos. CSIRT.

Cybersecurity ; Infrastructure Security Agency. (2021). Joint cyber defense collaborative. CISA.

Deep Instinct. (2021, 10 de febrero). Cyber Threat: Report on 2020 Shows Triple-Digit Increases across all Malware Types. Deep Instinct.

Deloitte. (2016, 12 de julio). Seven hidden costs of a cyberattack. Deloitte United States.

REFERENCIAS Y BIBLIOGRAFÍA

Deloitte. (2020, 9 de enero). 91% of all cyber attacks begin with a phishing email to an unexpected victim. Deloitte Malaysia.

El Mostrador Mercados (2020, 7 de septiembre). El lunes negro de Banco Estado: Gobierno admite "ataque cibernético muy profundo" y la Fiscalía inicia investigaciones con la PDI. El Mostrador.

El Mostrador. (2022, 24 de septiembre). Hackeo al Estado Mayor Conjunto: Monsalve confirma que ciberataque ocurrió en mayo de este año. El Mostrador.

Embroker Team. (2019, 18 de septiembre). 2022 must-know cyber attack statistics and trends. Embroker

European Commission. (2020, mayo). EU grants nearly €49 million to boost innovation in cybersecurity and privacy systems. Shaping Europe's Digital Future.

Feldman, S. (2019, 15 de enero). Infographic: No clear leader in cybersecurity market. Statista.

FortiGuard Labs. (2022, 8 de febrero). Reporte de ciberataques en América Latina. Fortinet.

Fortinet. (2022, marzo). Top cybersecurity statistics, facts, and figures for 2021. Fortinet.

Fortune Business Insights. Cyber security market overview by size, growth & trends, 2028. (n.d.). Recuperado el 27 de marzo, 2022, en

Gartner. (2021a, 17 de mayo). Gartner forecasts worldwide security and risk management spending to exceed $150 billion in 2021. Gartner.

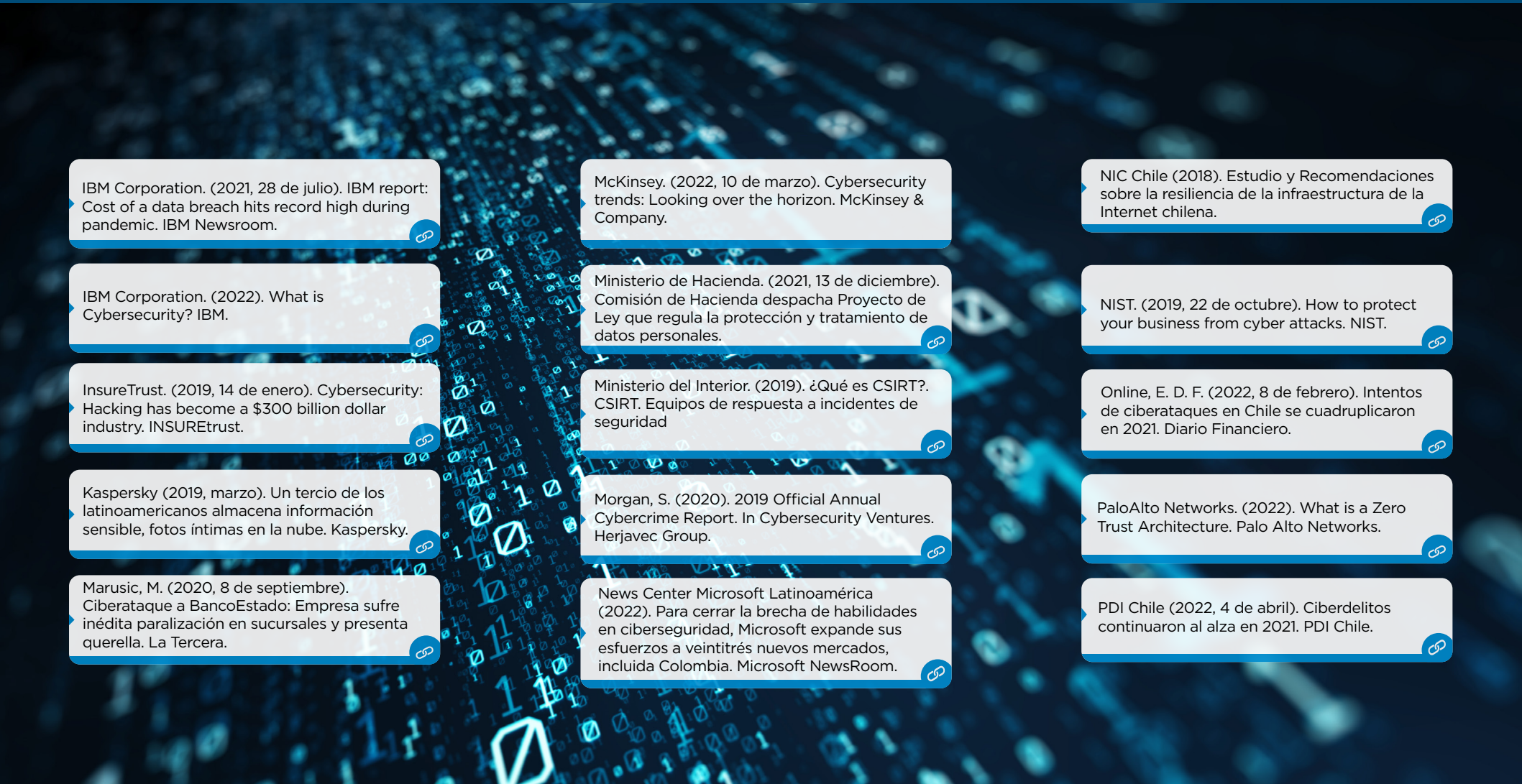
Gartner. (2021b, 20 de octubre). The top 8 cybersecurity predictions for 2021-2022. Gartner.

Gartner. (2022). Las principales tendencias tecnológicas estratégicas para 2022. Gartner.

Gobierno de Chile. (2017). Política nacional de Ciberseguridad 2017-2022.

González, C. (2022, 26 de septiembre). Ciberataque al Poder Judicial: Departamento de informática asegura que virus afectó al 1% de los computadores. Emol.

IBM Corporation. (2020). Cost of a Data Breach Report 2020. In IBM. IBM Security.



IBM Corporation. (2021, 28 de julio). IBM report: Cost of a data breach hits record high during pandemic. IBM Newsroom.

IBM Corporation. (2022). What is Cybersecurity? IBM.

InsureTrust. (2019, 14 de enero). Cybersecurity: Hacking has become a $300 billion dollar industry. INSUREtrust.

Kaspersky (2019, marzo). Un tercio de los latinoamericanos almacena información sensible, fotos íntimas en la nube. Kaspersky.

Marusic, M. (2020, 8 de septiembre). Ciberataque a BancoEstado: Empresa sufre inédita paralización en sucursales y presenta querella. La Tercera.

McKinsey. (2022, 10 de marzo). Cybersecurity trends: Looking over the horizon. McKinsey & Company.

Ministerio de Hacienda. (2021, 13 de diciembre). Comisión de Hacienda despacha Proyecto de Ley que regula la protección y tratamiento de datos personales.

Ministerio del Interior. (2019). ¿Qué es CSIRT?. CSIRT. Equipos de respuesta a incidentes de seguridad

Morgan, S. (2020). 2019 Official Annual Cybercrime Report. In Cybersecurity Ventures. Herjavec Group.

News Center Microsoft Latinoamérica (2022). Para cerrar la brecha de habilidades en ciberseguridad, Microsoft expande sus esfuerzos a veintitrés nuevos mercados, incluida Colombia. Microsoft NewsRoom.

NIC Chile (2018). Estudio y Recomendaciones sobre la resiliencia de la infraestructura de la Internet chilena.

NIST. (2019, 22 de octubre). How to protect your business from cyber attacks. NIST.

Online, E. D. F. (2022, 8 de febrero). Intentos de ciberataques en Chile se cuadruplicaron en 2021. Diario Financiero.

PaloAlto Networks. (2022). What is a Zero Trust Architecture. Palo Alto Networks.

PDI Chile (2022, 4 de abril). Ciberdelitos continuaron al alza en 2021. PDI Chile.

PwC. (2022, 1 de abril). Attractive cybersecurity subsidy for SMEs. PwC.

Reilly, D. (2021, 16 de noviembre). Cybersecurity experts say public-private partnership is the key to preventing future attacks. Fortune.

Sands, G. (2022, 2 de marzo). Senate passes major cybersecurity legislation to force reporting of cyberattacks and ransomware. CNN.

Scott, I. (2021, 17 de agosto). New US Infrastructure Bill Includes $1.9 Billion for Cybersecurity Funding, More Than Half Goes To State and Local Governments. CPO Magazine.

Senado de Chile (2022). Protección y tratamiento de datos personales: claves de la modernización en trámite. Senado de Chile.

Senado de Chile (2022). Noviembre será el mes dedicado a reflexionar sobre la infraestructura crítica de la información. Senado de Chile.

Senado de Chile (2022). Proyecto de ley, iniciado en Mensaje del ex Presidente de la República, señor Sebastián Piñera Echeñique, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.

SERCOTEC. (2022). Ciberseguridad.

SUBTEL (2021, 8 de junio). Mujeres, personas de bajos ingresos y con menores niveles educacionales presentan mayor brecha en el uso de servicios digitales. SUBTEL.

UK Cabinet Office. (2022, 27 de enero). Government cyber security strategy: 2022 to 2030 (HTML). GOV.UK.

U.S. Department of Homeland Security. (2022). SFS.

Vega, M. (2018, 21 de septiembre). Millonario hackeo al Banco de Chile se originó en computador de sucursal en Valdivia. Bio-Bio Chile.

Purplesec. (2020, 8 de noviembre). 2021 cyber security statistics trends & data. PurpleSec.

Hoja de Ruta de Ciberseguridad
Iniciativa impulsada por Microsoft y el Centro de Innovación UC
Primera edición / diciembre 2022

Equipo de desarrollo de contenidos, redacción y edición
Centro de Innovación UC Anacleto Angelini

Apoyo en redacción
Alejandra Reinoso

Videos
CACHALOTE

Fotografías
PhotoAdvisor.cl
Se agradece a quienes facilitaron imágenes para este documento

Diseño y diagramación
delacalle.cl

Portada
Marca Futuro

HOJA DE RUTA DE CIBERSEGURIDAD

SI QUIERES SABER MÁS DE ESTA INICIATIVA ESCRÍBENOS A
CENTRODEINNOVACION@UC.CL