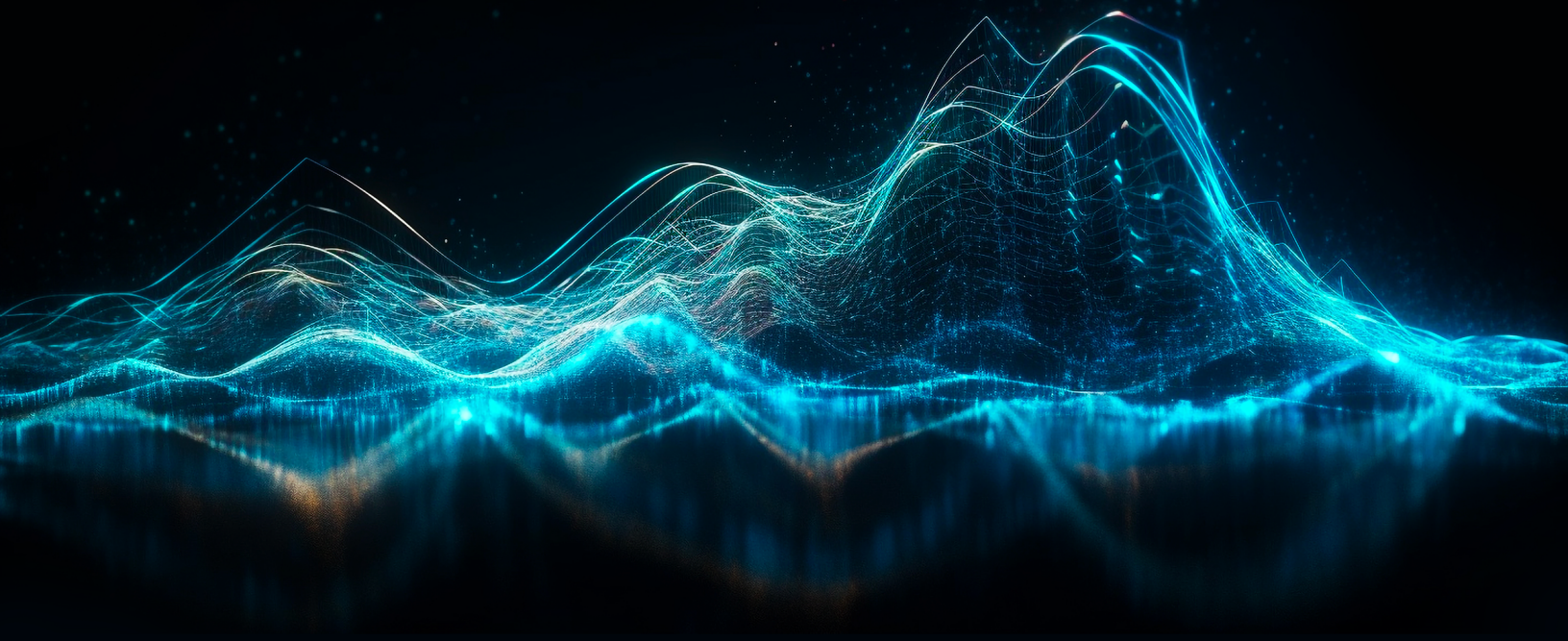
→CONSTRUYENDO LA CIBERSEGURIDAD EN CHILE←



→COMISIÓN DESAFÍOS DEL FUTURO, CIENCIA, TECNOLOGÍA E INNOVACIÓN←

Biblioteca del Congreso Nacional de Chile / BCN

Comisión Desafíos del Futuro, Ciencia, Tecnología e Innovación

Sr. Francisco Chahuán Chahuán, Presidente
Sra. Ximena Órdenes Neira, Senadora
Sra. Ximena Rincón González, Senadora
Sr. Kenneth Pugh Olavarría, Senador
Sr. Luciano Cruz-Coke Carvallo, Senador

I.S.B.N. 978-956-7629-62-6

Michael J. Heavey
Editor General

Tania Yovanovic, Raimundo Roberts, Carolina Muñoz, Pascal de Smet d´Olbecke
Editores adjuntos

Carolina Sancho, Pelayo Covarrubias, Xavier Bonnaire, Tania Yovanovic, Romina Torres, Pedro Pablo Pinacho, Rodrigo Alfaro, Luz Cardona, Eduardo Morales, Igor Carrasco, Jorge Gatica, Felix Staicu, Francisco Méndez, Carla Illanes, Julio Cámara, Kenneth Pugh
Editores

Aníbal J. Phillippi
Diseño Gráfico

Construyendo La Ciberseguridad en Chile- Mesa de Ciberseguridad de la Comisión Desafíos del Futuro, Ciencia, Tecnología e Innovación, 2022. Michael J. Heavey, Editor General, Valparaíso, Chile, Ediciones Biblioteca del Congreso Nacional de Chile 2023, 200 páginas

Senado-Chile
Comisión Desafíos del Futuro, Ciencia, Tecnología e Innovación – Senado Chile
Mesa de Ciberseguridad 2022


A1
INNOVATION
Data-A
A1
information

PREFACIO

El trabajo realizado por la mesa de Ciberseguridad marca un hito de colaboración para enfrentar un tema que nos afecta a todos en el mundo de la Cuarta Revolución Industrial, y que nos demanda los mejores esfuerzos para tener un país más seguro en el ciberespacio.

Se han analizado múltiples desafíos, de los que surgen importantes propuestas, que deben ser una poderosa guía para avanzar en la ciberseguridad y en las tecnologías emergentes que inciden en nuestra sociedad, y que sin duda producirán enormes cambios económicos y sociales, pero por sobre todo humanos.

El Senado de la República ha acogido muchas iniciativas a través de la Comisión de Desafíos del Futuro, que han sido base de nuevas legislaciones, y que han sido posibles por el concurso de especialistas y académicos, que en forma generosa han aportado su tiempo y experiencia para visibilizar temas que tienen un impacto en el desarrollo del país.

La ciberseguridad es, sin duda, una realidad de la que hace algunos lustros ni siquiera se hablaba, pasando a ser en la actualidad una piedra angular del futuro nacional, que camina a pasos agigantados hacia la transformación digital de nuestra sociedad. Por ello, debemos avanzar en el desarrollo de capacidades para desenvolvernos en escenarios que pondrán a prueba nuestras instituciones y su resiliencia, y por lo tanto nuestra democracia y forma de vida.

Considerando lo anterior y las recomendaciones del presente informe, impulsaremos desde el Senado la creación del "Foro Nacional de Ciberseguridad", siguiendo la experiencia de otras naciones con instancias similares. Este importante paso formalizará el constante interés de la institución en el impacto de las tecnologías emergentes y gravitantes, teniendo siempre como norte el bienestar futuro de la Nación.

Así planteado, el Foro será una instancia permanente, para convocar la colaboración de los mejores expertos, especialistas y conocedores provenientes no solo de la academia, sino también de la industria y las organizaciones de la sociedad civil, para que podamos trabajar sobre esta materia con la altura de miras que requiere tal desafío.

JUAN ANTONIO COLOMA CORREA
PRESIDENTE DEL SENADO DE LA REPÚBLICA DE CHILE

PRESENTACIÓN

La Ciberseguridad es un desafío constante de las sociedades modernas, donde la colaboración es la piedra angular para ser más resilientes en el ciberespacio, en el cual se desenvuelven hoy gran parte de nuestras actividades cotidianas.

Los países deben hacer importantes esfuerzos para abordar esta materia con una visión holística y con el debido sentido de urgencia, trabajando por nuevas legislaciones y normativas, innovando, educando y formando profesionales, pero por sobre todo creando una cultura en ciberseguridad que permita a todos sus habitantes obtener los beneficios de la cuarta revolución industrial en la que estamos inmersos.

Europa ha dado los pasos necesarios para consolidar la Ciberseguridad creando normativa, investigación y desarrollo, institucionalidad y gobernanza, tanto a nivel de sus miembros como de la comunidad, y que hoy permiten disponer, entre otras cosas, de un Centro Europeo de Ciberseguridad en Bucarest, Rumania, y una poderosa normativa actualizada denominada NIS2, para proteger infraestructura y entidades críticas, y la futura Ley de Ciber Resiliencia, para asegurarse que los productos conectados son seguros.

Miramos con mucho interés los pasos que da vuestro país en materias de ciberseguridad. Reconocemos el esfuerzo realizado a través del Senado de Chile, y que se reflejan en este documento que sin lugar a dudas servirá para un mejor conocimiento, entendimiento, mayor difusión cultura de ciberseguridad, pero por sobre todo un importante insumo para vuestra legislación y gobernanza en materias de ciberseguridad, y de transformación digital.

Felicitamos el esfuerzo de la academia chilena, la sociedad civil, los empresarios y profesionales que han trabajado en este documento. Miramos con perspectiva la formación del Foro Nacional de Ciberseguridad, con el cual esperamos tener una larga y fructífera relación que sea de mutuo beneficio.

MARGRETHE VESTAGER

Vicepresidenta Ejecutiva de la Comisión Europea

→COMISIÓN "DESAFÍOS DEL FUTURO, CIENCIA, TECNOLOGÍA E INNOVACIÓN"

Senadora
XIMENA ORDENES N.

Senador
KENNETH PUGH O.

PRÓLOGO

La experiencia lograda en el año 2021 al amparo de la Comisión de Transportes y Telecomunicaciones del Senado, que se tradujo en el Documento Chile Digital 2035, gracias a la participación de la Asociación de Empresas de Telecomunicaciones, junto a Cepal, la Academia y la Sociedad Civil, permitieron plantear una hoja de ruta en el proceso de transformación digital del País, con un horizonte a 12 años.

Dentro de las materias abordadas en dicho documento, destaca la inclusión de la Ciberseguridad, y durante el año 2022, como integrantes de la Comisión de Desafíos del Futuro, decidimos impulsar la Ciberseguridad como un eje relevante de nuestra mirada de futuro, considerando el alto y creciente impacto que tiene en nuestra sociedad.

Es así que convenimos en proponer y patrocinar la creación de una Mesa de Ciberseguridad, a objeto de convocar a un amplio espectro de profesionales desde la academia, la industria, las organizaciones civiles, las Fuerzas Armadas, las Fuerzas de Orden y Seguridad, así como a muchos profesionales con experiencia comprobada en estas materias.

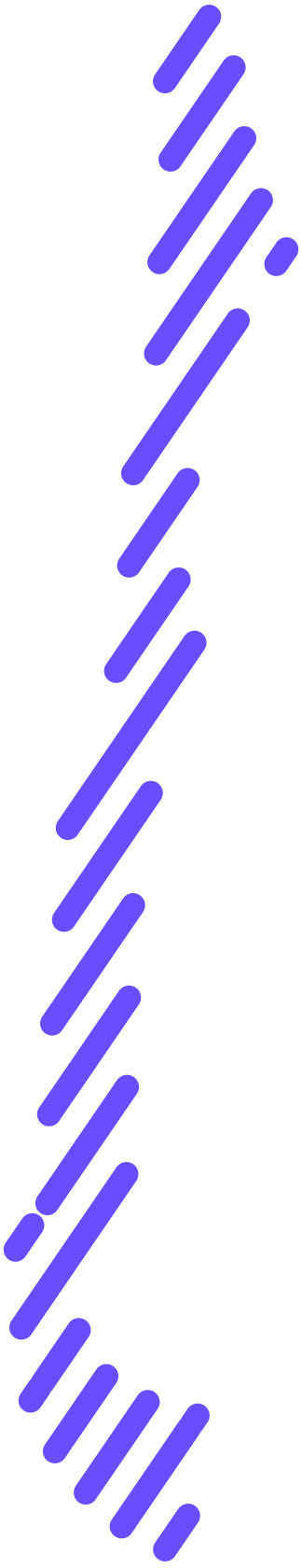
Lo hicimos con el propósito de ahondar sobre lo ya avanzado, y proponer nuevas alternativas y caminos para ser tomadas tanto por el Ejecutivo como el Legislativo y dar así un fuerte un impulso al desarrollo de la ciberseguridad nacional.

Agradecemos a los más de 140 profesionales que aceptaron el desafío de trabajar y disponibilizar su tiempo, cuyo esfuerzo suma varios miles de horas de trabajo, a fin de poner en la discusión los caminos a seguir para contar con una sociedad más familiarizada con la ciberseguridad, más resiliente y más innovadora, aprovechando de la mejor manera posible nuestras capacidades y talentos, a la vez de reconocer nuestras falencias y dolores.

Se abordaron diversas materias por parte de esta mesa, cuyo trabajo abarcó múltiples frentes y cuyo desarrollo y conclusiones se presentan en los capítulos siguientes.

Si de algo estamos seguros luego de este magnífico ejercicio, es de la necesidad de contar con un órgano formal y consultivo que convoque, al amparo del Senado, a especialistas, académicos, empresarios, sociedad civil y otros, a un foro permanente donde estas materias puedan ser canalizadas, donde se puedan plantear, conversar y discutir, de manera de nutrir el trabajo legislativo y normativo con la agilidad y profundidad que se requiere, y que nos permita así tomar y mantener una posición de vanguardia en Ciberseguridad.

El presente documento será un faro para el desarrollo de la ciberseguridad en Chile, basado en el principio de la colaboración necesaria entre todos, pues nadie está libre de vulnerabilidades que puedan ser explotadas maliciosamente.



INTRODUCCIÓN

La Comisión "Desafíos de Futuro, Ciencia, Tecnología e Innovación", además de cumplir con su labor legislativa, se ha consolidado como una instancia para poder generar prospectiva y tratar temas fuera de la contingencia política, sino con una mirada de futuro. De ella han surgido temas que incidirán ciertamente en el futuro de la nación, y que se condensan en el libro "Chile Tiene Futuro, desde sus Territorios", editado este año y que contiene las iniciativas abordadas desde su creación hasta el año 2021.

La creación de la Mesa de Ciberseguridad en esta Comisión fue una iniciativa promovida por la senadora Ximena Órdenes y el senador Kenneth Pugh, de manera de visibilizar los temas de ciberseguridad ya levantados en el informe de la Estrategia Chile Digital 2035 que se realizó al amparo de la Comisión de Transportes y Comunicaciones del Senado. Su propósito es el desarrollo de estas materias en un marco de amplia colaboración.

La mesa inició formalmente el 7 de Julio de 2022, en una sesión especial de la Comisión de Desafíos del Futuro (presidida por su presidente el Senador Francisco Chahuán) en la que se convocó a 140 especialistas provenientes de la academia, la industria, servicios públicos, Policías, Fuerzas Armadas, organizaciones civiles y otros profesionales focalizados en temas atingentes a ciberseguridad, transformación digital y políticas públicas, quienes aceptaron la invitación a participar y colaborar con su tiempo y esfuerzo.

El trabajo que se presenta aquí implicó un compromiso personal de muchas reuniones, y miles de horas hombre de trabajos, lecturas y conversaciones con el único propósito de aportar a esta iniciativa, comprometiendo tiempos personales y laborales, reconociendo el principio rector que rige a quienes nos desempeñamos en el rubro:

¡EN CIBERSEGURIDAD NO SE COMPITE, SE COLABORA!

Gracias a todos los que participaron en este gran proyecto.

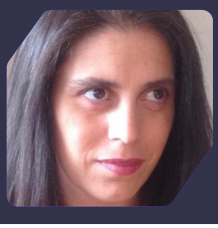
MICHAEL J. HEAVEY
Ingeniero Civil Electrónico
Coordinador de la Mesa Ciberseguridad
Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación
Valparaíso, Abril de 2023.

ORGANIZACIÓN DE LA MESA DE CIBERSEGURIDAD

La modalidad de trabajo fue principalmente virtual, aprovechando las ventajas de la tecnología. Y es así como entre los meses de julio y diciembre, se realizó esta importante labor que se condensa en los siguientes capítulos y que servirá de guía y de inspiración para los procesos de organización, gobernanza, normativa y legislación que el país necesita para proyectarse al futuro como una verdadera República Digital Cibersegura.

Tomando como base el capítulo de Ciberseguridad del documento Chile 2035, la mesa se organizó en 7 sub-mesas, las cuales se completaron según el interés personal de cada uno, y que fueron cada una dirigidas por un chair y un cochair

→01
Ciberseguridad y Políticas Públicas, a cargo de la **Dra. Carolina Sancho** y **Pelayo Covarrubias, Mag.**




→02
Desarrollo de Talento Ciber, a cargo del **Dr. Xavier Bonaire, y Tania Yovanovic.**


→03
Investigación Avanzada en Ciberseguridad, a cargo de la **Dra. Romina Torres** y **Dr. Pedro Pablo Pinacho.**

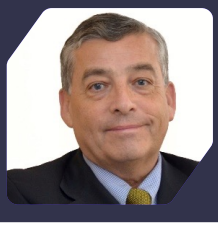

→04
Tecnologías Emergentes, a cargo del **Dr. Rodrigo Alfaro** y **Dra. Luz Cardona, Mag.**


→05

Operadores de Servicios Esenciales, a cargo del **Ing. Eduardo Morales** y **Igor Carrasco, Mag.**


→06

Desinformación en Línea, a cargo del **Dr. Jorge Gatica** y **Félix Staicu, MsSc.**

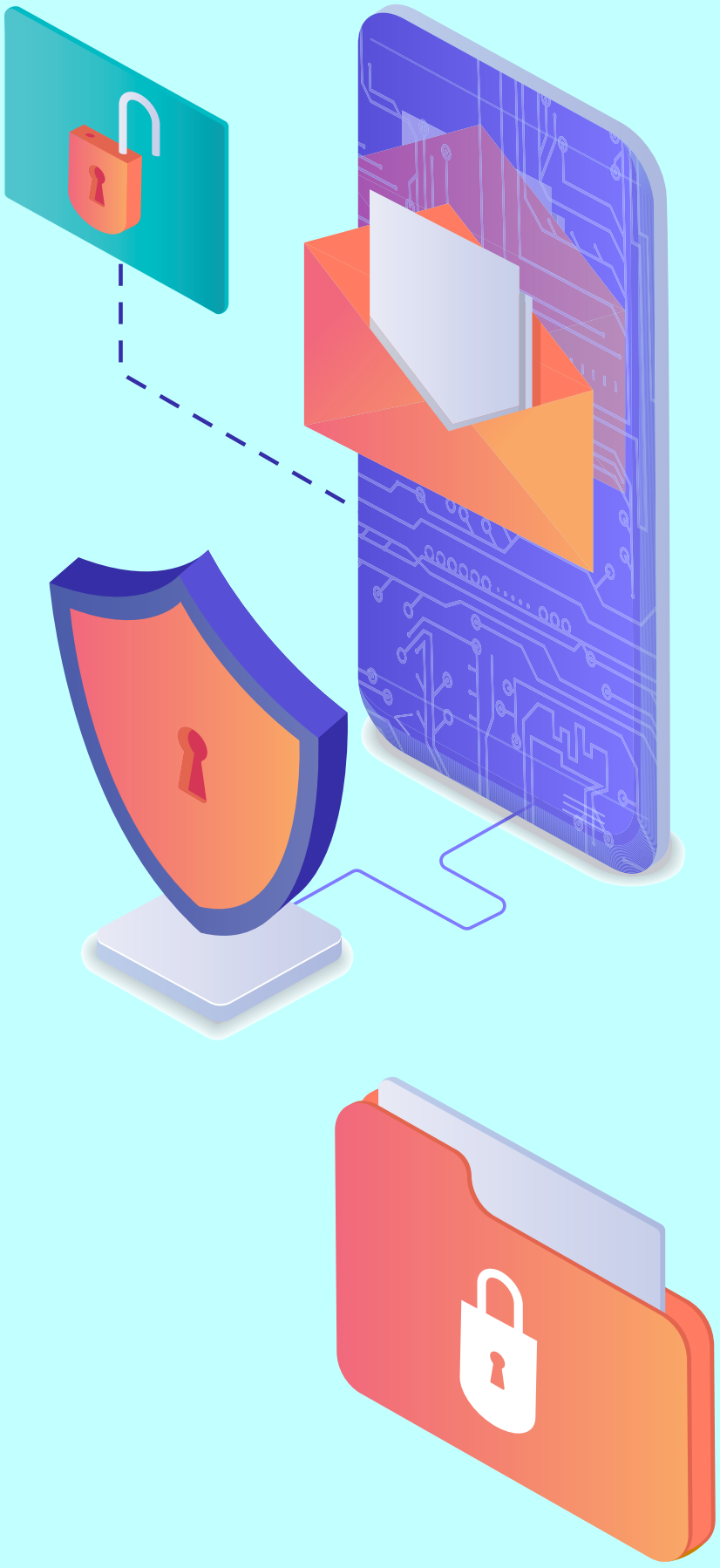



→07

Interoperabilidad e Identidad Digital, a cargo de **Francisco Méndez, Mag.,** y **Carla Illanes, Mag.**


→08

Foro Nacional de Ciberseguridad



CONVOCADOS A LA MESA DE CIBERSEGURIDAD

→Alberto Jara	→Gabriel Bergel	→Monica Retamal
→Alejandro Hevia	→Gonzalo Díaz de Valdés	→Pablo Itaim
→Alex Pessó	→Guillermo Carey	→Paola Arellano
→Alexandra Barros	→Guillermo Garcia	→Patricia Diaz
→Alfie Antonio Ulloa	→Héctor González	→Patricio Leyton
→Alfredo Diaz	→Helvecia Castro	→Patricio Ovalle
→Amalia Pizarro	→Hernan Espinoza	→Paula Pinto
→Andrea Obaid	→Igal Neiman	→Paulina Silva
→Andres Barrientos	→Ingrid Inda	→Pedro Huichalaf
→Andrés Pumarino	→Italo Foppiano	→Pedro José Novoa
→Benjamín Blanco	→Jaime Astorquiza	→Peter Waher
→Berioska Contreras	→Jaime Caiceo	→Puppy Rojas
→Carlos Bustos	→Javier Ramírez	→Raúl Arrieta
→Carlos Fuentes	→Jessica Matus	→Renato Bustamante
→Carlos Lobos	→Jorge Arredondo	→Ricardo Andrade
→Carlos Manzano	→Jorge Astudillo	→Ricardo Dorado
→Carlos Montoya	→Jorge Flores	→Ricardo Monreal
→Carlos Parker	→Jorge Rojas	→Ricardo Seguel
→Carmina Hernandez	→José Fuentealba	→Ricardo Soto
→Catherine Narváez	→Jose Luis Perez	→Ricardo Vásquez
→César Galindo	→Juan Carlos Ramirez	→Rocío Ortiz
→César Pallavicini	→Juan Huechucura	→Rodrigo Bustamante
→Christian Sifaqui	→Juan Ignacio Nicolossi	→Rodrigo Díaz
→Claudia Inostroza	→Juan Lopizic	→Rodrigo Pérez
→Claudia Negri	→Juan Pablo Gonzalez	→Rodrigo San Martin
→Claudio Álvarez	→Julio Lopez	→Romina Garrido
→Claudio Galleguillos	→Karin Quiroga	→Ruth Garrido
→Claudio Reyes	→Kristian Araoz	→Sebastian Berrios
→Cristián Rojas	→Lidia Herrera	→Sebastián Carey
→Danic Maldonado	→Loreto Bravo	→Sebastián Izquierdo
→Daniel Álvarez	→Luis Silva	→Sebastián Vargas
→Daniel Seco	→Marcelo Wong	→Sergio Leiva
→Daniel Velásquez	→Marco Zuniga	→Taryn Revesz
→Daniela Rusowsky	→Maria Francisca Yañez	→Thierry de Saint Pierre
→Diego Philippi	→María José Escobar	→Victoria Hurtado
→Edison Escobar	→Mario Troncoso	→Ximena Cisternas
→Eduardo Costoya	→Marisel Cabeza	→Ximena Sepulveda
→Felipe Rodríguez	→Mauricio Cantergiani	→Yerka Yukich
→Fernanda Mattar	→Mauricio Romo	→Pamela Calisto
→Fernando Mejías	→Maurizio Mattoli	→Cristian Rojas
→Fernando Muñoz	→Michelle Bordachar	→Paz Suarez
→Francisco Correa	→Miguel Cisterna	→Carolina Muñoz
→Francisco Garcia	→Miguel Solís	→Felipe Rodríguez
→Freddy Macho	→Mirko Koscina	→María Paz Ilabaca

RESUMEN EJECUTIVO

El informe de la Estrategia "Chile Digital 2035", en lo relativo a la ciberseguridad, señala en su párrafo inicial:

"No se puede avanzar en transformación digital sin una adecuada estrategia de ciberseguridad. Chile debe, conforme con su propia realidad, establecer políticas y medios que permitan la protección de sus activos informáticos y de comunicaciones, así como su resiliencia frente a eventuales vulnerabilidades o fallas".

Sobre la premisa anterior, la Mesa de Ciberseguridad trabajó aportando insumos para estrategias de seguridad, con muchas bajadas y propuestas que permitan, en una forma holística, visualizar los dolores, las necesidades, los caminos y oportunidades que nos permitan ir madurando en ciberseguridad como país.

Enfrentar lo anterior requiere de reconocer algunos aspectos importantes de los pasos que estamos dando. Chile cuenta con una Política Nacional de Ciberseguridad de 2017 -2022 con 25 objetivos y 43 medidas, que han sido una hoja de ruta para enfrentar el desafío de la ciberseguridad. Disponemos de una ley que consagra a Octubre como el Mes de la Ciberseguridad, lo que ha permitido ir posicionando el tema en la mente de los chilenos.

También hemos avanzado en modernizar nuestra regulación mediante la Ley N° 21.459 que "Establece normas sobre delitos informáticos, deroga la ley n° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest", siendo un importante avance. Por otra parte, se está avanzando en una legislación Marco de Ciberseguridad y Operadores Esenciales y Críticos de la Información, así como en regular la protección de datos personales.

Por otra parte, la Academia ha tomado medidas para preparar nuevos profesionales que se hacen cada vez más necesarios para atender requerimientos de organizaciones de todo tamaño. Junto a la creación de carreras de pregrado en la especialidad, se desarrollan otros estudios de post grado en materias afines. Pero el camino es largo y la formación de hábitos de ciberhigiene, detección de talentos y reducción de las brechas de alfabetismo digital son desafíos permanentes.

Es interesante constatar un internalización de la importancia de la ciberseguridad, tomándose cada vez más conciencia de nuestra enorme dependencia de la Internet, de los sistemas de información y todo lo que ello conlleva en nuestro diario desempeño.

Algunos recientes eventos de ciberseguridad comprometieron, aunque sin mayores consecuencias, importantes activos informáticos lo que ha generado una sana preocupación, y por supuesto ocupación en la materia, reconociendo así la tremenda vulnerabilidad que tenemos como país en el ciber espacio.

Con todo lo anterior, estamos construyendo un marco jurídico de la ciberseguridad en el cual falta camino por recorrer, pero, a través de iniciativas como esta mesa, el país va reduciendo brechas y vulnerabilidades, madurando nuestra Ciberseguridad.

Marco jurídico de Ciberseguridad

Fuente: Equipo Legislativo Senador Kenneth Pugh

El trabajo de la mesa convocada, se subdividió en 7 submesas , estas fueron:

1) **Ciberseguridad y Políticas Públicas.**

2) **Desarrollo Talento Ciber**

3) **Investigación Avanzada en Ciberseguridad**

4) **Tecnologías Emergentes,**

5) **Operadores de Servicios Esenciales,**

6) **Desinformación en Línea,**

7) **Interoperabilidad e Identidad Digital**

Las 7 submesas partieron de un análisis de la realidad nacional en cada tema, sobre una estructura similar, es decir: Introducción, Contexto, Desafíos Futuros, Propuestas y Conclusiones. Estas entregaron sus correspondientes informes en el mes de diciembre de 2022 proveyendo importantes visiones e insumos de la futura evolución de la ciberseguridad en nuestro país para los próximos años. Se reflejan dolores, aspiraciones, y necesidades ineludibles que van desde marcos reglamentarios apropiados hasta una gobernanza que permita una participación segura y robusta de nuestro país en el ciberespacio.

Las submesas concluyen, de forma similar, en conceptos como la necesidad de una Política robusta, la profundización de la transformación digital del Estado, la necesidad de una gestión del cambio y la necesaria creación de gobernanzas apropiadas, sin dejar de promover la educación y formación en ciberseguridad. Estos temas, desarrollados en mayor o menor profundidad según la materia de cada grupo, señalan una importante convergencia de lo que se considera relevante en la ciberseguridad nacional.

El trabajo de este equipo de especialistas no se agota al finalizar la Mesa convocada por la Comisión Desafíos del Futuro, sino se proyecta hacia la creación de un "foro permanente" , con el auspicio del Senado, destinado a ser un órgano consultivo y voluntario donde se puedan canalizar inquietudes e iniciativas que permitan lograr mejores legislaciones y normativas actualizadas en este ecosistema que avanza a pasos agigantados.

Concluye así el trabajo de la mesa con la descripción de lo que será el "Foro Nacional de Ciberseguridad".

ÍNDICE

005 PREFACIO

007 PRESENTACIÓN

009 PRÓLOGO SENATORIAL

011 INTRODUCCIÓN

012 ORGANIZACIÓN DE LA MESA DE CIBERSEGURIDAD

015 CONVOCADOS A LA MESA DE CIBERSEGURIDAD

016 RESUMEN EJECUTIVO

022 Capítulo 1_**Ciberseguridad y Políticas Públicas**

023 INTRODUCCIÓN

024 CONTEXTO

025 DESAFÍOS FUTUROS

029 PROPUESTAS

033 CONCLUSIONES

034 Capítulo 2_**Desarrollo Talento Ciber**

035 INTRODUCCIÓN

035 CONTEXTO EN CHILE

036 RANKING DE CIBERSEGURIDADAD

040 DESAFÍOS

043 DESARROLLO Y PROPUESTAS

063 CONCLUSIONES

064 Capítulo 3_**Investigación Avanzada en Ciberseguridad (IAC)**

065 INTRODUCCIÓN

066 CONTEXTO

072 SITUACIÓN BASE DEL PAÍS EN IAC

075 SITUACIÓN FUTURA

076 PROGRAMA DE INICIATIVAS PRIORITARIAS

086 Capítulo 4_**Tecnologías emergentes en ciberseguridad para Chile**

087 INTRODUCCIÓN

087 CONTEXTO

094 DESAFÍOS FUTUROS

097 PROPUESTA

102 Capítulo 5_**Operadores de Servicios Esenciales**

103 INTRODUCCIÓN

104 CONTEXTO EN CHILE
105 ANÁLISIS DE ENTORNO Y ESTÁNDARES EN IICCY SSEE EN CHILE
106 BRECHAS Y RECOMENDACIONES DE SEGURIDAD EN IICC Y SSEE
110 DEFINICIONES Y PROPUESTA DE SECTORES ESTRATÉGICOS
113 PRINCIPALES LINEAMIENTOS ESTRATÉGICOS PROPUESTOS
125 PRINCIPALES CONCLUSIONES Y RECOMENDACIONES

128 Capítulo 6_ **Estrategia Nacional Contra la Desinformación en Línea**
129 INTRODUCCIÓN
131 CONTEXTO: EL ALCANCE DEL TÉRMINO DESINFORMACIÓN
137 LA SITUACIÓN ACTUAL EN CHILE
141 ACTORES INVOLUCRADOS
144 PROPUESTA DE UNA ESTRATEGIA NACIONAL CONTRA LA DESINFORMACIÓN EN LÍNEA
147 CONCLUSIONES

148 Capítulo 7_ **INTEROPERABILIDAD E IDENTIDAD DIGITAL**
149 INTRODUCCIÓN
151 CONTEXTO
153 MODELO DE GOBERNANZA
155 MARCO REGULATORIO DE LA INTEROPERABILIDAD E IDENTIDAD DIGITAL EN CHILE HOY
160 ENTORNOS DE TRABAJO DE INTEROPERABILIDAD
164 ENTORNOS DE TRABAJO DE IDENTIDAD DIGITAL
185 GENERACIÓN DE VALOR POR LA INTEROPERABILIDAD E IDENTIDAD DIGITAL
190 GESTIÓN DEL CAMBIO: EJE DEL ÉXITO
198 DESAFÍOS FUTUROS

202 Capítulo 8_ **El Foro Nacional de Ciberseguridad**
203 INTRODUCCIÓN
204 OBJETIVOS DEL FORO NACIONAL DE CIBERSEGURIDAD
206 FORMALIZACIÓN DEL FORO
207 CONFORMACIÓN EJECUTIVA DEL FORO
207 DE LA MEMBRESÍA DEL FORO
208 DE LAS MESAS DE TRABAJO
211 FUNCIONAMIENTO DE LAS MESAS DE TRABAJO

*Capítulo 1_*

Ciberseguridad y Políticas Públicas

PARTICIPARON EN LA ELABORACIÓN DE ESTE TEXTO:

- Equipo Coordinador submesa "Ciberseguridad y Política Pública": Carolina Sancho y Pelayo Covarrubias.

- Comité de Trabajo Técnico de la submesa "Ciberseguridad y Política Pública" convocado por la Comisión formado por: Sebastián Izquierdo, Marisel Cabeza, María Francisca Yañez, Alberto Jara, Jessica Matus, Paola Arellano, Paulina Silva, Romina Garrido, Carmina Hernández, Hernán Espinoza, Daniel Álvarez, Jaime Astorquiza, Íngrid Inda, Pedro Huichalaf, Catherine Narváez, Juan Pablo González, Edison Escobar, Michel Souza, Michelle Bordachar y Claudia Inostroza.

1. INTRODUCCIÓN

La transformación digital de nuestra sociedad gracias a la Tecnologías de la Información y Comunicaciones es una realidad ineludible. Junto a ella, la ciberseguridad, un concepto que hace algunos decenios era inexistente, es un tema de permanente preocupación donde el Estado debe tomar un rol de liderazgo y regulador , por medio de la accion articuladora y normativa.

La creciente automatización, robotización y digitalización, así como ha traído enormes beneficios, también ha generado nuevos desafíos, de los cuales nuestro país no está exento; muy por el contrario, estamos con rezago respecto de paises líderes del mundo occidental y de la OCDE. Por este motivo, es necesario avanzar en términos de mejorar y establecer una estructura legal y normativa que permita asegurar un desarrollo más robusto y resiliente en el ciberespacio, dotando de las herramientas apropiadas para disponer de una ciberseguridad adecuada, según los estándares internacionales.

Se han dado pasos importantes que comienzan con establecimiento de la primera Política Nacional de Ciberseguridad 2017-2022 (PNCS), y que han permitido visibilizar la ciberseguridad y sensibilizar a la comunidad. Asimismo, ha traido como respuesta un correlato creciente en iniciativas legislativas en materias como delitos informáticos y protección de datos, a las que se suman la creación de organismos y entidades públicas como el "CSIRT de Gobierno", y próximamente la Agencia Nacional de Ciberseguridad.

En el marco de este desafío constante y creciente que es la ciberseguridad, se convocó a veintidos profesionales, entre abogados, empresarios, ingenieros, periodistas y otros a conformar la mesa de trabajo denominada **"Ciberseguridad y Políticas Públicas"**, los cuales desde el 30 de junio de 2022 hasta el 5 de enero de 2023 y mediando más de 5 reuniones plenarias y muchas horas de trabajo durante el período con el objeto de analizar y proponer cambios al marco regulatorio, presentan en este capitulo diversas propuestas a ser consideradas por los legisladores para mejorar nuestra el tratamiento del tema de la ciberseguridad desde una óptica de política publica, fortaleciendo nuestra realidad en la materia, y muy especialmente en la legislación.

2. CONTEXTO

El legislativo ha evidenciado, un rol insustituible en la regulación de asuntos vinculados con la seguridad en el ciberespacio, lo que ha implicado la actualización de leyes. Por ejemplo, en el caso del delito informático y el avance que ha significado pasar de la Ley Nº 19.223/1993 a la Ley Nº 21.459/2022 como compromiso de Chile al adherirse al Convenio de Ciberdelincuencia (Convenio de Budapest). A lo cual se adiciona el esfuerzo que se lleva a cabo para contar próximamente con una institucionalidad especializada en el tema, es decir, una Agencia Nacional de Ciberseguridad.

El ejecutivo, tiene un rol clave en el tema por su papel de responsable primario en la respuesta a problemas públicos, a través de políticas públicas, que contemplan entre otras medidas la promoción de una regulación de asuntos que en ciberseguridad se relacionan, por ejemplo, con la infraestructura crítica y la infraestructura crítica de la información, la protección de datos personales, planes de continuidad de negocios, entre otros.

La formulación de una política pública en ciberseguridad no sólo involucra al sector público. El sector privado, dueño de la mayor cantidad de infraestructura crítica asociada al ciberespacio, como también, desde el ambiente académico, desde donde se detectan en forma incipiente problemas, dilemas y desafíos, son actores que requieren ser considerados activamente cuando es abordado el tema de la ciberseguridad como respuesta a los peligros que existen el uso del ciberespacio.

Adicionalmente, pero no menos importante, la sociedad civil a través del ciudadano y/o en forma organizada desde entidades especializadas que contribuyen en la formulación de insumos y demandas que el Ejecutivo requiere considerar en el marco de un sistema político democrático, donde la participación e inclusión son principios que guían su actuación ante la ciudadanía.

3. DESAFÍOS FUTUROS

Identificar los desafíos a considerar, en el caso chileno en materia de ciberseguridad bajo una perspectiva de política pública, ha sido una tarea compleja por tratarse de materias diversas y su articulación para una mejor comprensión y dimensionamiento del esfuerzo que se requiere. Con la finalidad de facilitar la sistematización de ellos, son desarrollados a partir de los objetivos planteados en la PNCS (Política Nacional de Ciberseguridad 2017-2022)

3.1 OBJETIVO 1 PNCS: "El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos".

Desafío(s):

Disponer de Ley Marco de Ciberseguridad, que considere:
El fortalecimiento de la gestión de riesgos, planes de continuidad del negocio para asegurar los componentes que puedan ser atacados o expuestos y que afecten la continuidad operacional de los servicios y la implementación de estándares internacionales en el tema, otorgando así, confianza y seguridad, en las instituciones públicas como privadas que operan en el ciberespacio.

Que contemple un trabajo multidisciplinario que concilie una acción especializada e integral, evitando pensar en una lógica exclusivamente técnico. Su aprobación, permitiría el establecimiento por mandato legal de una arquitectura de ciberseguridad, su funcionamiento y modo en que se relacionará con otras entidades o actores involucrados en el marco de la gestión de esta agencia gubernamental.

Establecer la necesaria institucionalidad que permita la interacción entre los CSIRT de los diferentes sectores como públicos y privado, favoreciendo y fortaleciendo la coordinación oportuna entre ellos ante un incidente o prevención de éste, especialmente en ciertos sectores especialmente críticos.

Colocar especial énfasis en el elemento de cultura o concientización como aspecto clave para generar cambios al interior de las organizaciones (Gestión del Cambio). De esta manera, alcanzar exitosamente este desafío, aportará claridad en términos de quién tiene atribuciones y competencias para regular, coordinar, fiscalizar y sancionar; cuando ocurran incidentes de ciberseguridad.

También, establecerá una conceptualización en términos de lo que entenderá por sector regulado, sus características que permitan considerarlo como tal y quienes serán considerados como sujetos obligados.

Nota: *A la fecha de este informe (abril 2023) se encuentra en primer trámite constitucional, la ley marco de ciberseguridad Boletin 14.847-06, cuyas indicaciones están siendo revisadas por las Comisiones Unidas de Seguridad y Defensa del Senado En ella se recogen una importante proporción de lo señalado en este punto.*

3.2 OBJETIVO 2 PNCS: "El Estado velará por los derechos de las personas en el ciberespacio".

Desafío(s):

Considerar el sistema de ciberseguridad como un todo, no como regulaciones aisladas. Las certezas necesarias para los mercados regulados, para las personas, empresas, entidades públicas vienen de la mano con el avance paralelo, homogéneo de las distintas iniciativas que permitan establecer claramente "las reglas del juego" en esta materia.

El avance en la ley de delitos informáticos, por mencionar un caso, exigirá ajustes a las empresas en sus modelos de prevención de delitos implementados en virtud de la ley 20.393. Estos ajustes significan en la práctica avanzar hacia modelos integrales de gobernanza de datos, sobre todo de los datos personales y sensibles, que permitan establecer sistemas de control efectivos para salvaguardarlo. Así para la implementación de esta ley, son necesarias directrices que contenidas en las leyes de protección de datos personales (estándar mínimo) y además dependiendo del sector regulado, si corresponde a un servicio crítico y/o esencial de la infraestructura crítica de la información, la ley marco de ciberseguridad también contempla obligaciones precisas para los sujetos obligados (ej. Sector público y aquellas instituciones declaradas como críticas u operadores vitales).

Teniendo en cuenta que el derecho a la seguridad informática es una condición habilitante para el ejercicio de otros derechos, es necesario dar especial seguimiento a que las políticas, leyes y prácticas de ciberseguridad, estén encaminadas a la defensa y promoción del derecho a la privacidad, acorde a los deberes asumidos por el Estado de Chile en diversos tratados internacionales de derechos humanos, tales como: Artículo 12, Declaración Universal de los DDHH; Artículo 17, PIDCP; Artículo 16, Convención sobre los Derechos del Niño; Artículo 5, Declaración Americana de los Derechos y Deberes del Hombre; Artículo 11.2, Convención Americana sobre DDHH.

Favorecer que todas las personas estén en condiciones de disfrutar de sus derechos y libertades fundamentales en el entorno digital, por este motivo, se deben crear las circunstancias necesarias para eliminar las situaciones de discriminación, abuso y violencia que afectan mayoritariamente a algunos sectores de la población. Para lo anterior, es necesario que en la racionalidad de la elaboración de programas, proyectos y acciones dirigidos a la protección de la seguridad informática se dé prioridad a la protección de quienes se encuentran en situación de desventaja, especialmente mujeres, niños, niñas y adolescentes, personas de la tercera edad, y personas con discapacidades.

3.3 **Objetivo 3 PNCS: "Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales".**

Desafío(s):

Promover una cultura en materia de ciberseguridad que contribuya a enfrentar las contingencias en el sector público y privado, y resguardar la seguridad de las personas en el ciberespacio.

La educación de la ciberseguridad es la piedra angular en los procesos seguros de transformación digital, donde todos los ciudadanos son potenciales usuarios y deben considerar no solo desde las edades escolares tempranas, básicas y medias, sino procesos continuos, reconociendo el constante cambio.

Considerar la promoción de la ciberhigiene o higiene digital que permita la creación de hábitos y buenas prácticas en el manejo de los sistemas informáticos y dispositivos móviles en toda la población, y en especial en las instituciones públicas y el ambiente educacional.

Potenciar la colaboración y alianzas público-privadas, para un mejor intercambio de información y conocimiento en asuntos relacionados con la ciberseguridad, pero también fomentar la creación de conocimiento asociado a estas materias. Colaborar en ciberseguridad no es óbice para la competencia en los mercados.

Incorporar enfoque etario en la ciberseguridad teniendo presente que dependiendo de la edad cambian los intereses, características de las medidas y niveles de seguridad a promover.

3.4 Objetivo 4 PNCS: "El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales".

Desafío(s):

Avanzar en la formulación y promulgación de una política internacional para el ciberespacio.

Evaluar la necesidad permanente de adaptación de la institucionalidad vigente para considerar los desafíos que implica estar inmersos en este ecosistema, así como la protección de activos relacionados con los sistemas de información, procesamiento, datos y redes. Avanzar en una visión holística de inserción en el ciberespacio, reconociendo y adoptando estándares internacionales.

Promover, sistematizar y monitorear eficazmente los acuerdos de cooperación que desde el ejecutivo se firmen o se han firmado en materia de ciberseguridad, que permita identificar las oportunidades y limitaciones para hacer uso de estos acuerdos, en caso de ser necesarios por los encargados pertinentes.

3.5 Objetivo 5 PNCS: "El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos".

Desafío(s):

Promover la unificación normativa, debido a que se necesita poner fin a la dispersión normativa de estos últimos años, dónde existen varios estándares distintos para la industria.

Entrega de lineamientos y/o recomendaciones para el sector privado respecto a lo que deben tener en ciberseguridad una pequeña, mediana y gran empresa, por ejemplo, en lo relacionado con sistemas de prevención y detección.

Promover una industria de ciberseguridad, que responda a las necesidades nacionales, particularmente en lo relacionado con las necesidades estratégicas e inclusive permita la exportación y/o integración de estos desarrollos tecnológicos al exterior.

4. PROPUESTAS

Se propone la formulación de nuevos objetivos, los cuales corresponden a:

4.1 NUEVO OBJETIVO A: "Propender a que la política pública de ciberseguridad favorezca una gobernanza en la materia, facilitando la inclusión de sectores, área y expertos en la materia, generando instancias para las diferentes categorías de aportes".

Su inclusión permitiría:

- Contar con un requisito habilitante para la transformación digital, para el resguardo de información y la protección de los datos personales, en definitiva, para el ejercicio de los derechos y la vida de las personas en el mundo digital.

-Promover y fortalecer la convergencia, coordinación y articulación público-privada, condición necesaria, más no suficiente para la gestión de alertas preventivas y de incidentes de ciberseguridad.

-Contemplar un modelo de institucionalidad pública, con principios orientadores de: coordinación, particularmente con el sector privado de manera permanente. Toda vez que, al mejorar las instancias de comunicación, coordinación y colaboración entre diversas instituciones, organizaciones y empresas, tanto del sector público como privado, nacionales e internacionales se facilita la oportuna detección de un incidente en el ciberespacio e inclusive su contención. Además, es importante contar con la participación de la academia para incorporar las tendencias internacionales en estas materias y el conocimiento existente en torno a un asunto en particular, entre otros beneficios.

- Implementar en base a una institución de características similares a la Comisión Futuro del Senado, una instancia patrocinada por este que puede denominarse como "Foro Nacional de Ciberseguridad", la que fungiría como entidad consultiva, prospectiva y propositiva en materias de legislación sobre ciberseguridad.

- Favorecer una gobernanza en ciberseguridad, que al menos debiera contemplar: una institucionalidad pública que se coordine con el sector privado de manera permanente, para garantizar la seguridad en el ciberespacio, que ayude a prevenir; una orgánica definida en sus roles; una autoridad con competencias robustas; el incremento de profesionales especializado/as y existan políticas para la retención del talento; disponibilidad de presupuestaria en la programación anual, considerando los requerimientos y contingencias a lo largo de todo el año; posibilidad permanente de capacitación a funcionarios y funcionarias, desde donde el sector privado/academia puedan colaborar con dicha formación de talento.

4.2 NUEVO OBJETIVO B: "Profundizar la transformación digital del Estado"

Su inclusión permitiría:

- Facilitar la implementación de la ley de transformación digital, que también requiere requisitos habilitantes de base que deben observar las mismas normativas (Ley marco de ciberseguridad, en cuanto a que todos los servicios estatales se consideran esenciales/críticos). Además, es necesario actualizar la ley de protección de datos personales, y el Decreto Supremo N° 83/2005, sobre norma técnica para los órganos de administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

- Establecer una ley de gobernanza de la interoperabilidad para el Estado, que establezca la regulación sobre la forma de compartir información que posee el mismo, sin necesidad de estar requiriéndola permanentemente (Principio de solo una vez).

- Establecer las políticas de administración del cambio dentro del Estado para facilitar el uso de la información, estableciendo normas y reglas sobre como acceder a la información y data, los enfoques de privacidad que incluyan la anonimización de datos, entre otras.

- Robustecer la identidad digital de manera que los procesos de identificación, autenticación y validación aseguren que la información accedida solo lo sea por quien está habilitado para ello (es efectivamente quien dice ser).

- Robustecer la firma electrónica y su aplicación universal

- Establecer el uso del domicilio digital universal, donde la persona pueda ser notificada o pueda mantener su relación informativa con el Estado.

- Avanzar en el desarrollo de la ficha médica universal

4.3 NUEVO OBJETIVO C: "Promover una PNCS con enfoque multisectorial"

Su inclusión permitiría:

- Facilitar el involucramiento de las partes interesadas, incluidas las organizaciones de la sociedad civil, de una manera holística y sostenida para obtener resultados de políticas públicas mejor informados y basados en evidencia.

- Formulación a partir de un intenso diálogo público - privado, con representantes de servicios públicos, organizaciones gremiales y la sociedad civil, además de académicos y expertos nacionales e internacionales.

- Contemplar que el borrador de la segunda versión de la PNCS pase por un proceso de consulta pública, al igual que la primera versión hoy vigente.

4.4 NUEVO OBJETIVO E: "PNCS con enfoque de género e impacto social"

Su inclusión permitiría:

- Tener especial consideración que algunas formas de violencia digital son dirigidas mayoritariamente en contra de las mujeres y requiere de un monitoreo especial, por ejemplo, es posible identificar Gendertrolling: define a un tipo de usuario especialmente indignado con la idea de que las mujeres opinen; Acoso en línea (cyberharassment): Acto de provocar en forma intencional un malestar emocional a la víctima de carácter sustancial, a través de expresiones en línea persistentes, de modo que formen parte de un curso de acción, y no sean solamente un incidente aislado; Hostigamiento en línea (cyberstalking):

Continuación del hostigamiento físico por medios digitales, esto es, el seguimiento reiterado de una persona a través de internet u otros medios electrónicos (como por ejemplo, cámaras de vigilancia, dispositivos de escucha electrónicos, software para computadores o aplicaciones para celulares, y dispositivos GPS), incluyendo conductas tales como el envío de comunicaciones no deseadas, avances o peticiones de carácter sexual, amenazas de violencia, y la vigilancia o monitoreo de la localización de la víctima, sus actividades cotidianas y/o sus comunicaciones; Creepshot: Se refiere a una foto tomada por un hombre a una mujer o niña en público sin su consentimiento. Las fotos suelen centrarse en los glúteos, las piernas o el escote de la víctima; Cyberflashing: Envío de fotografías obscenas a una mujer sin su consentimiento con el objetivo de molestarla, intimidarla o incomodarla.

- Fomentar el estudio que aborde el impacto de usar el ciberespacio en la vida cotidiana, bajo un enfoque holístico, desde en diferentes disciplinas académicas como por ejemplo, la sicología, sociología, ciencia política, relaciones internacionales, derecho, economía y pedagogía, entre otras. Considerando especialmente cómo el uso frecuente de los medios digitales afecta las relaciones personales y sociales de los ciudadanos. Asimismo, contemplar los efectos de las RRSS y medios en la creación y difusión de información falsa (fake news), errónea (misinformación) o manipulada que se orienta a distorsionar los hechos que presenta (desinformación) estimulando el desarrollo de la capacidad de los ciudadanos de distinguir estos casos de la información veraz, confiable y fidedigna.

- Dar especial seguimiento y atención de este asunto, promoviendo una estadística oficial y pública que dé cuenta de la evolución de esta situación.

4.5 NUEVO OBJETIVO E: "PNCS con enfoque etario"

Su inclusión permitiría:

Considerar medidas a implementar de acuerdo a las características de cada etapa de la vida de las personas, teniendo presente que cada una de estas tienen un nivel de conocimiento, acercamiento a la tecnología, intereses, exposición, responsabilidad y problemáticas muy distintas. Este enfoque debiera estar presente en forma transversal a toda la política. Considerar el contexto de grupos vulnerables, como por ejemplo, adultos mayores, por quienes debe considerarse una atención en lugares físicos a sus necesidades virtuales.

5. CONCLUSIONES

El texto desarrollado es resultado de un trabajo interdisciplinario de expertos y expertas en ciberseguridad. Identifica los desafíos actuales derivados de los objetivos establecidos en la actual PNCS y sugiere propuestas como resultado de la evaluación del contexto en el cual se plantea en 2017 los objetivos de la PNCS, como, asimismo, considerando la evolución observada de aquellos. Se pretende hacer un aporte al trabajo del legislativo en su insustituible rol de regulación jurídica de la ciberseguridad, como también, al ejecutivo y sus organismos especializados, especialmente cuando se está en el inicio de la formulación de la segunda versión de la PNCS.

Desde una perspectiva de los desafíos identificados, es necesario profundizar el trabajo iniciado en términos de fortalecimiento de la seguridad del ciberespacio desde una óptica de gestión de riesgos. Asimismo, es necesario avanzar en la protección de los derechos de las personas en el ciberespacio, como también, promover ampliamente una cultura de prácticas seguras en el uso del ciberespacio por parte de ciudadanos e incrementar la formación de expertos en ciberseguridad, considerando el déficit que existe en Chile en el tema. Además, es necesario avanzar en la política internacional chilena del ciberespacio. Finalmente, es necesario conectar la industria con las necesidades mínimas de ciberseguridad según estándares internacionales en su funcionamiento, como también, promover una capacidad nacional que permita generar el desarrollo tecnológico que nuestro país requiere en el tema, contemplando la posibilidad de exportarlo.

En cuanto a las propuestas futuras, por un lado, es necesario enfocar la política pública de ciberseguridad desde una óptica de la gobernanza, estimulando la coordinación interagencial y considerando criterios de inclusividad. Por otro lado, una nueva versión de la política de ciberseguridad, requiere un enfoque de género, e impacto social considerando las situaciones diferencias que afecta a las personas, y en especial a las mujeres en el ciberespacio y la necesidad de capacitación para incorporarlas en los avances tecnológicos y expectativas de desarrollo. Por otra parte, se plantea la necesidad de considerar al ciudadano en sus diferentes edades, dado que sus características debieran enfocar cada medida a desarrollar, de modo que efectivamente se orienten a las personas.

*Capítulo 2_*

Desarrollo Talento Ciber

PARTICIPARON EN LA ELABORACIÓN DE ESTE TEXTO:

- Equipo Coordinador submesa "Desarrollo Talento Ciber": Xavier Bonaire y Tania Yovanovic

- Comité de Trabajo Técnico de la submesa "Desarrollo Talento Ciber" convocado por la Comisión formado por: Ximena Sepúlveda, Martin Seguel, Rodrigo San Martin, Alexandra Barros, Sebastian Vargas, Lidia Herrera y Claudia Jaña.

1. INTRODUCCIÓN

El Ciberespacio es una creación integra del ser humano; es el resultado de una creación colectiva que se expande a ritmo vertiginoso, y que en su proceso va demandando nuevos aportes y desarrollo de conocimientos. El ciberespacio demanda nuevos talentos, y estos deben detectarse desde edad temprana, dar las facilidades para su desarrollo y formación, y su colocación en el mercado.

La demanda es enorme, en países europeos se reconocen importantes déficit presente y futuro, y ello se extrapola fácilmente a nuestra realidad nacional. En consecuencia, estamos frente a una realidad que demanda una atención permanente, con nuevas estrategias y acciones que permitan desarrollar nuestro talento ciber y ponerlo a disposición para resolver las necesidades del país.

En más de 20 reuniones de trabajo, entre sesiones plenarias y de grupos de trabajo, desarrolladas entre el 22 de junio y el 30 de noviembre de 2022, un equipo conformado de profesionales de formaciones diversas entre los que se cuentan abogados, ingenieros, periodistas, empresarios y académicos, lograron el resultado que se refleja en este capítulo.

2. CONTEXTO EN CHILE

La ciberseguridad en un tema preocupante en Chile, tanto en el ámbito de los organismos estatales como con respecto a las empresas privadas. La gran cantidad de eventos recientes, con ataques a instituciones y empresas que son parte de la infraestructura crítica del país, refleja en sí mismo la falta de una cultura general en ciberseguridad en Chile, y en algunos casos, la falta de preocupación por el tema.

Las diferentes crisis de ciberseguridad evidenciadas públicamente durante 2022, indican una falta de preparación del país no solamente en cuanto al uso de tecnología adecuada, sino que también por el manejo, en ocasiones inadecuado, de estas crisis.

El sentido común nos lleva a pensar que la ciberseguridad es esencialmente un problema técnico donde se trata de usar la tecnología correcta, en el lugar correcto y al momento correcto. Sin embargo, la ciberseguridad es primero un asunto humano.

Humanos intervienen en toda la cadena de la ciberseguridad, desde el diseño de sistemas y programas (software) seguros, la implementación de tecnología como los cortafuegos o los sistemas de detección y prevención de ataques, la repuesta a incidentes y el análisis forense, hasta la gestión de crisis con la comunicación y otras acciones asociadas.

En este contexto, el desarrollo de talentos ciber en Chile debe ser parte de un plan global de mejora de la ciberseguridad nacional. El déficit que el país registra de especialistas en ciberseguridad implica una gran dificultad para los organismos estatales y las empresas para contratar profesionales en el tema. El desarrollo de talentos ciber es entonces una prioridad para mejorar el nivel global del país en esta materia.

3. RANKING DE CIBERSEGURIDAD

La evaluación del estado de un país en ciberseguridad es fundamental para poder remediar las eventuales debilidades encontradas y generar políticas y acciones adecuadas para eliminarlas. Existen varios estudios a nivel mundial para estimar el estado en la materia para los países. En general, los resultados obtenidos suelen ser un poco diferentes para un país entre una u otra clasificación, pero eso se debe a la no uniformidad de los criterios que se usan para la evaluación en cada clasificación. Las clasificaciones más reconocidas por la comunidad en ciberseguridad son:

La clasificación de la International Telecommunication Union - ITU, organismo de la ONU que genera una clasificación de todos los países miembros cada dos años.

La clasificación National Cybersecurity Index de la e-Governance Academy en Estonia.

3.1 ITU - Cybersecurity Index

La ITU (International Telecommunication Union), organismo de la ONU (Naciones Unidas) emite cada dos años una clasificación en ciberseguridad de todos los países que son parte de la organización. El estudio se realiza a partir de los datos entregados por los países miembros alrededor de 5 pilares de la ciberseguridad:

- Medidas Legales: Mide el estado actual de un país en función de las medidas legales y las regulaciones existentes, incluyendo las leyes sobre la ciberdelincuencia, leyes de protección de datos y la regulación de las infraestructuras críticas.

· Medidas Técnicas: Mide el estado actual del país en función de la implementación de medidas técnicas a través de agencias nacional y regionales, incluyendo un CERT/CSIRT en actividad tanto a nivel estatal que sectorial, y mecanismos de protección y reporte en caso de abuso infantil.

· Medidas Organizacionales: Mide las estrategias y la organización a nivel nacional en la implementación de la ciberseguridad. Incluye la existencia de políticas nacionales de ciberseguridad, las agencias de ciberseguridad y las estrategias e iniciativas para la lucha en contra de los acosos infantiles en línea.

· Capacidad de Desarrollo: Mide el estado del país en términos de campañas de concienciación sobre la ciberseguridad, la existencia de ejercicios de ciberseguridad, la educación y la capacidad de desarrollo en el tema. Incluye la existencia de programas de Investigación e Innovación en ciberseguridad, así como la existencia de una industria en ciberseguridad.

· Cooperación: Mide la existencia de programas de cooperación entre agencias, entre empresas privadas y estatales, y con otros países. Incluye los acuerdos públicos/privados y los acuerdos bilaterales o multilaterales con otros países.

Monaco	72.57	69
Uzbekistan	71.11	70
Jordan	70.96	71
Uganda	69.98	72
Zambia	68.88	73
Chile	68.83	74
Côte d'Ivoire	67.82	75
Costa Rica	67.45	76
Bulgaria	67.38	77
Ukraine	65.93	78

Figura 1 - Ranking ITU Global - Chile 2021

Country Name	Overall Score	Regional Rank
United States of America**	100	1
Canada**	97.67	2
Brazil	96.6	3
Mexico	81.68	4
Uruguay	75.15	5
Dominican Rep.	75.07	6
Chile	68.83	7
Costa Rica	67.45	8
Colombia	63.72	9
Cuba	58.76	10

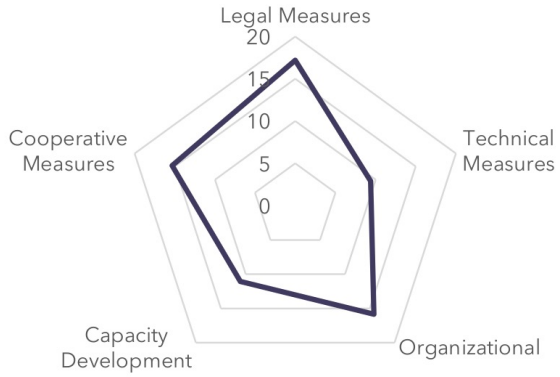
Figura 2 - ITU Ranking Regional 2021

Basados en los resultados obtenidos en estos 5 indicadores, la ITU genera una clasificación con un puntaje entre 0 y 100 para cada país.

En clasificación del año 2021, Chile se encuentra en la posición 74 a nivel mundial con un puntaje de 68.83 según se aprecia en Figura 1, pero bastante lejano de los 10 primeros países de la clasificación que muestra la Figura 3. Sin embargo, existe un avance de varios lugares desde el informe anterior del 2019.

A nivel regional, Chile se encuentra en el séptimo lugar, con una mejor evaluación que Colombia, Perú, Argentina y Paraguay, pero detrás de Brasil, México, Uruguay y República Dominicana. La Figura 2 muestra la ubicación de Chile a nivel regional.

Chile



Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
68.83	17.20	9.39	15.84	11.07	15.33

Source: ITU Global Cybersecurity Index v4, 2020

Figura 4 - Ranking ITU Chile 2021 - Desglose de puntaje

La Figura 3 muestra el puntaje que obtuvo Chile en los 5 indicadores de Cybersecurity Index de la ITU en 2020. Se nota que los dos indicadores donde Chile demuestra los mejores resultados son en Medidas Legales y en Medidas Organizacionales. Este resultado se explica por el avance del país en la creación de nuevas leyes en el ámbito de la ciberseguridad, como la última sobre los ciberdelitos.

Sin embargo, en los ítems correspondientes a las medidas técnicas (Technical Measures) y a las capacidades de desarrollo, el país muestra un atraso bastante importante. El ítem de capacidades de desarrollo incluye la capacidad de Chile para desarrollar talentos ciber, y más específicamente la capacidad de educación en ciberseguridad en el país.

3.2 Ranking NCSI – National Cyber Security Index

El ranking NCSI es la segunda clasificación internacional de referencia en ciberseguridad. Está publicado por la e-Governance Academy. Fundada en 2002, la e-Governance Academy (eGA) es una fundación sin fines de lucro: una iniciativa conjunta del Gobierno de Estonia, el Open Society Institute (OSI) y el Programa de las Naciones Unidas para el Desarrollo.

NCSI national cyber security index

50. Chile 59.74

Population	18.2 million
Area (km²)	756.1 thousand
GDP per capita ($)	25.4 thousand

50th	National Cyber Security Index	60 %
74th	Global Cybersecurity Index	69 %
56th	ICT Development Index	66 %
44th	Networked Readiness Index	57 %

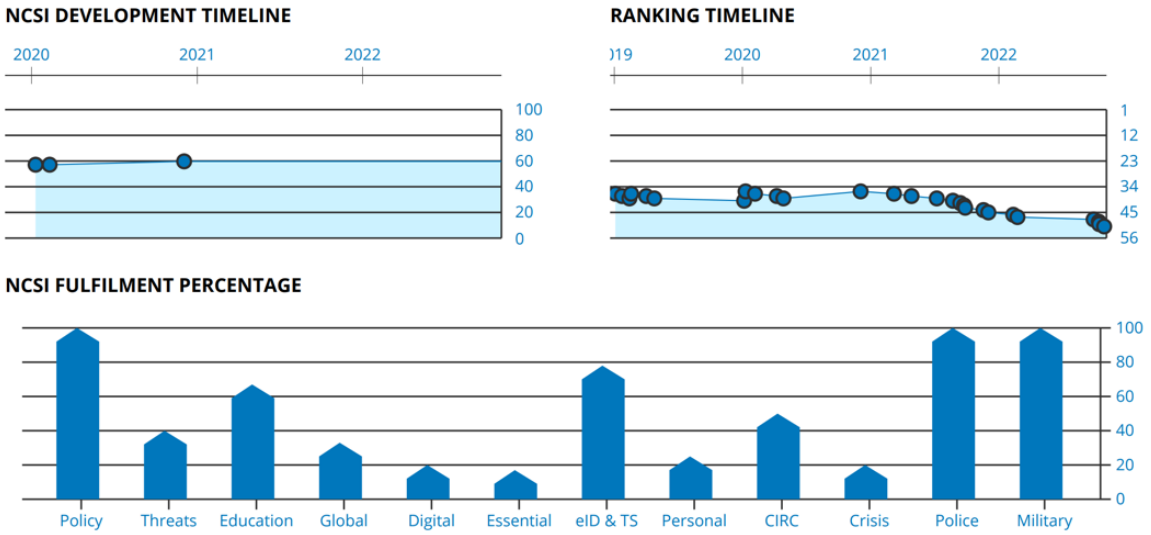


Figura 5 - Ranking NCSI - Chile 2022

Lo significativo, es que Chile bajó 13 lugares en este ranking entre el año 2019 y noviembre 2022. Esto se debe principalmente a los siguientes factores:

1. La cantidad importante de crisis de ciberseguridad que Chile tuvo que enfrentar durante este periodo, y especialmente durante los últimos meses, con una serie de eventos relacionados con organizaciones estatales. El puntaje refleja también la falta de un manejo apropiado de la crisis en ciberseguridad tanto a nivel estatal como privado, debido a la falta de profesionales calificados para esta tarea.

2. Un déficit importante de personal en ciberseguridad, directamente relacionado con el desarrollo de talentos ciber y las capacidades del país en educación en ciberseguridad, que sea educación temprana, superior o continua.

3. Una casi ausencia de normativas adecuadas para el manejo de datos personales, lo que tiene como consecuencia una alta tasa de filtración de estos datos.

Aunque se puede destacar un gran avance en los aspectos legales de la ciberseguridad durante los últimos años, y especialmente con la nueva ley N°21449 sobre los delitos informáticos, el ranking NCSI, al igual que el de la ITU, muestra claramente las deficiencias del país en materia de ciberseguridad.

4. DESAFÍOS

El documento Estrategia de Transformación digital "Chile Digital 2035", estableció dos objetivos que dicen relación con lo que hemos denominado **"Desarrollo de Talento Ciber"**:

OBJETIVO 2 Cultura integral de ciberseguridad nacional

· Desarrollar programas de ciber higiene en la sociedad para menores de edad a partir de los 2 y hasta los 12 años.

· Desarrollar programas de formación en habilidades digitales orientadas a la ciberseguridad durante toda la formación escolar.

· Crear programas que mitiguen la violencia en redes desde edad temprana y hagan frente a situaciones de ciberacoso en menores.

· Desarrollar programas de acompañamiento digital a Adultos Mayores para mitigar riesgos a los que son expuestos en el Ciberespacio

OBJETIVO 3 Gestión del Talento, desarrollo de capacidades y de industria de ciberseguridad

· Ejecutar programas para identificar y desarrollar ciber talentos a partir de los 14 años.

· Desarrollar habilidades digitales entregando competencias certificadas para alumnos de todas las edades a partir de los 18 años y sin ser requisito de ingreso una formación académica previa, usando la metodología francesa de la Escuela 42.

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

· Fomentar el desarrollo de becas de postgrado en Ciberseguridad, en universidades de alto prestigio mundial, para doctorados y postdoctorados.

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

· Premiar anualmente a las mujeres destacadas en Ciberseguridad.

· Reconocer anualmente a las y los líderes emergentes destacados de la Ciberseguridad

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

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

Sobre la base de estos objetivos se plantean 4 aspectos a desarrollar, que se detallan a continuación:

Educación Básica y Media

· Educación temprana en ciberseguridad

· Habilidades digitales orientadas a ciberseguridad durante la formación escolar.

· Programas para mitigar la violencia en redes y ciberacoso de menores.

· Programas paras desarrollar e identificar talentos ciber a partir de los 14 años.

Educación Superior

· Mayor oferta educativa en ciberseguridad.

* Acreditación de competencias a través de estándares internacionales
* Para carreras técnicas y universitarias

· Formaciones que entregan títulos o grados

* Programas de pregrado (Ingeniería, Técnico, Profesional)
* Magister, Doctorado y Post-Doctorado

· Habilidades digitales y certificación de competencias para alumnos mayores de 18 años sin requisito de formación académica previa (modelo Escuela 42 en Francia).

· Fomento al desarrollo de becas de postgrado en ciberseguridad en universidades de alto prestigio.

· Formación e incorporación de mujeres a carreras de ciberseguridad para hacerse cargo de la brecha existente.

Educación Continua

· Sensibilización o Evangelización a la comunidad (ciudadanía en general)

· Programas de formación y acompañamiento a Adultos Mayores.

· Diplomas y certificaciones.

· Capacitación a empresas y organizaciones estales.

· Reconversión laboral.

· Programas alternativos al Servicio Militar para la formación de especialistas en Ciberdefensa.

Temas transversales

Contribuyen al desarrollo general de talentos en ciberseguridad.

· Creación del INCIBER (Instituto Nacional de Ciberseguridad)

* Concienciación.
* Acreditación de competencias.
* Organización de ejercicios nacionales de ciberseguridad.

· Premiar anualmente a las mujeres destacadas en ciberseguridad.

· Reconocer a las y los líderes emergentes y destacados en ciberseguridad.

· Colaborar en ciberseguridad entre el ámbito civil y las entidades de la defensa

* Proyectos de tecnología duales (civil + militar).
* Recursos adecuados para su ejecución.

5. DESARROLLO Y PROPUESTAS

Unos de los factores que explican el bajo nivel de ciberseguridad en Chile es la falta de educación temprana en este tema, y especialmente la ausencia de la enseñanza de las buenas prácticas en ciberseguridad en los colegios (**ciberhigiene**).

Publicaciones recientes, como el artículo del World Economic Forum destacan la necesidad de enseñar la ciberseguridad de forma temprana por dos razones:

1.Los niños usan dispositivos de tecnología (celulares, Tablet, computadores, consolas de juego,...) de forma cada vez más temprana, lo que los expone a riesgos de ciberseguridad y a riesgos cognitivos (ver informe de la OCDE).

2.Los niños y adolescentes son los blancos de muchos tipos de ciber-ataques

En este contexto, es necesario avanzar en la educación temprana en Ciberseguridad en Chile, con el fin de generar una conciencia nacional en la materia, por lo cual se desarrollan 7 Propuestas para este ciclo:

Propuesta 1 - Incluir la ciberseguridad como materia en el programa de enseñanza de educación básica y media

Es necesario incluir a la ciberseguridad como una materia propia de la enseñanza básica y media en los colegios y así generar una conciencia temprana de en los niños en sobre esta materia. El objetivo es enseñar las buenas prácticas en ciberseguridad en el uso de los celulares, de las redes sociales, de la gestión básica de credenciales (identificador de usuario + contraseña) y de los riesgos asociados a la exposición de datos personales.

Acciones a corto plazo

***Realizar charlas en los colegios y/o en las universidades y centros de educación superior para formar a los profesores en las buenas prácticas en ciberseguridad.
FINANCIAMIENTO: PÚBLICO/ PRIVADO

***Realizar campañas de parte del Ministerio de Educación en los medios de comunicación para sensibilizar a los niños y los padres en las buenas prácticas en ciberseguridad.
FINANCIAMIENTO: PÚBLICO

*Modificar el programa de la carrera de pedagogía para incluir una formación en ciberseguridad para los futuros profesores.
FINANCIAMIENTO: PÚBLICO

Acciones a mediano plazo

*Determinar el alcance y profundidad de las temáticas que se apliquen en cada nivel, además de las exigencias de implementación de las temáticas en las aulas de cada entidad educativa existente en el alcance de la propuesta. Revisar ejemplo tangible de países que hoy lideran en este ámbito, p.e. España.
FINANCIAMIENTO: PÚBLICO/ PRIVADO

Acciones a largo plazo

*Incluir la ciberseguridad en el programa de ciencias para profesores de educación básica y media.

*Definición de las Asignaturas por nivel creadas/actualizadas de acuerdo con la propuesta sobre los currículos.
FINANCIAMIENTO: PÚBLICO / PRIVADO

IMPACTOS ESPERADOS

· Sensibilizar a los profesores de colegios en los temas de ciberseguridad

· Sensibilizar a los niños en las buenas prácticas en ciberseguridad

· Sensibilizar a los padres en las buenas prácticas en ciberseguridad

· Generar una capacitación a los profesores como parte de los conocimientos adquiridos durante la carrera de pedagogía.

· Activar el desarrollo/modificación de las asignaturas seleccionadas, basado en las necesidades detectadas a nivel nacional por nivel.

· Activar la estructura de formación actualizada en colegios, escuelas y liceos del país.

Propuesta 2 - Cultura nacional en ciberseguridad en establecimientos educacionales.

Generar una Cultura Nacional en temas de ciberseguridad en padres, apoderados, profesores y alumnos.

Acciones a corto plazo

*Generar una Cultura Nacional en temas de ciberseguridad en padres, apoderados, profesores y alumnos de los distintos niveles educativos, desde la enseñanza básica hasta la media.
FINANCIAMIENTO: PÚBLICO

Acciones a mediano plazo

*Sensibilización a docentes en colegios, liceos respecto de las temáticas de Ciberseguridad.
FINANCIAMIENTO: PÚBLICO

Acciones a largo plazo

*Formación de monitores para liderar la actualización a docentes, padres y apoderados. Identificar líderes de los estamentos educativos que sean los guías del proyecto, de forma que mantengan actualizados a los encargados de cada nivel de acción, manteniendo viva y actualizada la temática de ciberseguridad.
FINANCIAMIENTO: PÚBLICO

IMPACTOS ESPERADOS

· Toma de conocimiento de los riesgos y beneficios de manejar temas de ciberseguridad a niveles de usuarios, accesos, cuentas seguras, manejo de claves, etc.

· Fomentar la actualización continua del conocimiento en la temática en cada una de las distintas entidades de educación.

· Crear cuerpos docentes preparados en la temática, de manera que estos apoyen a los alumnos y apoderados en la comprensión de la problemática y la solución de esta.

· Comunidad participativa y además con conocimiento actualizado respecto de la temática.

Propuesta 3 - Establecer alianzas de Formación y Actualización

Relacionar el mundo educativo con entidades formadoras y con experiencias reconocidas a nivel nacional.

Acciones a corto plazo

*Reconocer en el marco nacional las entidades de formación orientados a potenciar la generación de talentos para el mundo digital, para apoyar la transición de Chile a un país de la era digital.
FINANCIAMIENTO: PÚBLICO

Acciones a mediano plazo

*El Estado deberá ser parte de la formación de estas alianzas con un rol de aval de los vínculos generados, con el propósito de afianzar la relación y cubrir las necesidades de formación.
FINANCIAMIENTO: PÚBLICO/PRIVADO

Acciones a largo plazo

*Generar instancias de actualización constante mediante eventos, competencias y actividades desarrolladas en cada uno de los niveles educativos.
FINANCIAMIENTO: PÚBLICO /PRIVADO

IMPACTOS ESPERADOS

· Alianzas de calidad que beneficien el cambio y mejoramiento educativo en el ámbito de ciberseguridad.

· Fomentar la participación de los distintos sectores con el objeto de lograr la alianza necesaria para nuestros educandos.

· Interacción educación - empresa en pro de la educación en ciberseguridad, en educandos de las distintas edades en enseñanza básica y media.

Propuesta 4 - Diseñar programas de Formación Continua para Profesores

Diseñar programas de formación continua para profesores, tanto en ejercicio, recién egresados y estudiantes de las Carreras de Pedagogía. Educar a los futuros profesores del país, incluyendo en su currículo la ciberseguridad, considerando una actualización continua, permitiendo así construir una cultura nacional de seguridad cibernética.

Acciones a corto plazo

*Encuestar docentes en distintos niveles que estarían en condiciones de ser parte de esta propuesta, creando un catastro de los que serán parte de esta acción
FINANCIAMIENTO: PÚBLICO/PRIVADO

Acciones a mediano plazo

*Establecer, de acuerdo con dicho catastro, las etapas de concienciación que permitan cubrir las necesidades básicas de cada centro educacional, básico y/o medio.
FINANCIAMIENTO: PÚBLICO/PRIVADO

*Generar además documentación estándar para nivelar los conceptos a nivel nacional, de forma tal que no exista ambigüedad en el conocimiento a entregar.
FINANCIAMIENTO: PÚBLICO / PRIVADO

Acciones a largo plazo

*Establecer un plan de trabajo nacional a ser aplicado en cada región, ya sea mediante cursos presenciales o usando las tecnologías disponibles. En primera instancia guiados por profesionales expertos y tomando ejemplo de otros países como por ejemplo España, siendo este caso el más real y cercano a nuestra idiosincrasia.
FINANCIAMIENTO: PÚBLICO /PRIVADO

IMPACTOS ESPERADOS

· Que el país cuente con una fuerza de profesionales de la educación, que incorporen a su acción educativa las acciones necesarias para establecer conciencia en Ciberseguridad, logrando que las mentes en crecimiento adopten como suyo las prácticas de ciberhigiene necesarias para ser parte del mundo en el que se han de desarrollar.

Propuesta 5 - Formular un Programa de Certificación en Ciberseguridad

Formular un programa de acreditación de competencias y certificaciones en temas de ciberseguridad para profesores de enseñanza básica y media, de manera de asegurar un estándar de calidad en la entrega de los conocimientos. Validación de la calidad del conocimiento instaurado en docentes, verificando si este cumple con los conocimientos mínimos para ser parte de este proceso de alfabetización para cubrir la brecha digital.

Acciones a corto plazo

*Identificar Instituciones/Organizaciones con las que se pueda alcanzar a cubrir la población de docentes en forma regional y como país.
FINANCIAMIENTO: PÚBLICO/PRIVADO

Acciones a mediano plazo

*Creación de talleres de preparación y nivelación contemplando temas básicos de la tecnología, ciberhigiene, ya sea en forma presencial y/o virtual para los docentes que formen parte de esta acción.
FINANCIAMIENTO: PÚBLICO/PRIVADO

Acciones a largo plazo

*Creación del plan de certificaciones a nivel país apoyado en casos probados herramientas reconocidas como seguras, tanto para el establecimiento de contactos como para la medición de conocimientos que permita al grupo de profesionales optimizar el tiempo de aprendizaje.
FINANCIAMIENTO: PÚBLICO /PRIVADO

IMPACTOS ESPERADOS

· Profesores acreditados y certificados. Conocimientos y lenguaje unificado.

· Ciberhigiene digital actualizada. Trabajo en equipo entre el mundo privado y el público.

· Activación de convenios con IES, Empresas tecnológicas, Organismos de la Administración del Estado, ONGs, entre otras.

Propuesta 6 - Diseño de Programas y Campañas de Formación

Diseñar programas y campañas de formación de padres y apoderados con buenas prácticas en ciberseguridad (participación IES – Colegios – PDI – MINEDUC). Diseñar campañas de actualización para los docentes activos. Propiciar el conocimiento tecnológico que precisan hoy los padres, apoderados docentes activos que trabajan con los alumnos de esta generación tecnologizada.

Acciones a corto plazo

*Levantar la cantidad de entidades educativas que precisan actualizar a sus docentes en temas de Ciberseguridad.

*Levantar la cantidad de entidades educativas en las que se deben aplicar estas campañas, de manera de definir el alcance de esta propuesta. Generar el mapa de acción por región a trabajar.
FINANCIAMIENTO: PÚBLICO/PRIVADO

Acciones a mediano plazo

*Definición de las temáticas bases en las que se deben profundizar de acuerdo con la información adquirida en el punto anterior.
FINANCIAMIENTO: PÚBLICO/PRIVADO

Acciones a largo plazo

* Generar y accionar los cambios necesarios en las mallas curriculares con miras al objetivo inicial, acorde al sello de cada institución, con miras en el mejoramiento continuo.
FINANCIAMIENTO: PÚBLICO /PRIVADO

IMPACTOS ESPERADOS

· Logro de información clara tanto en profesorados como en entidades educativas con necesidades de actualización en los temas de Ciberseguridad.

· Padres, Apoderados y docentes preparados en las temáticas de higiene en ciberseguridad apoyando la formación del futuro de Chile.

· Capital humano fortalecido y preparado para la formación de nuestros futuros ciudadanos.

Propuesta 7 - Crear una certificación digital obligatoria para los alumnos de colegios y liceos

Las competencias en el mundo digital son cada vez más importantes para los ciudadanos, y en particular para que los jóvenes tengan conocimientos y capacidades mínimas en el tema, incluyendo ciberseguridad y buenas prácticas. Algunos países, como por ejemplo Francia con el programa PIX, ya han implementado, no solamente la enseñanza de estas buenas prácticas, sino que también su evaluación obligatoria para todos los alumnos de los colegios y liceos (que sean de enseñanza general o profesional). El programa PIX está alineado con las recomendaciones de la Unión Europea en términos de competencias digitales.

Acciones a corto plazo

*Diseñar un programa comparable al programa PIX en Francia para la enseñanza de las buenas prácticas de uso de las herramientas digitales.

* Formar a los profesores de los colegios para la enseñanza relacionada al programa (ver Propuesta 1 - Propuesta 2 - Propuesta 4 -)
FINANCIAMIENTO: PÚBLICO

Acciones a mediano plazo

*Diseñar una prueba de evaluación de capacidades digitales para los alumnos de colegios.
FINANCIAMIENTO: PÚBLICO

Acciones a largo plazo

*Implementar la prueba de evaluación de capacidades digitales para todos los alumnos de colegios.
FINANCIAMIENTO: PÚBLICO

IMPACTOS ESPERADOS

·Mejora sensible del nivel de buenas prácticas en el uso de las herramientas digitales de parte de la ciudadanía.

·Mejora sensible de uso de las buenas prácticas en ciberseguridad y ciberhigiene para la ciudadanía, y especialmente en la gestión de datos personales.

4.2 EDUCACIÓN SUPERIOR

El desarrollo de cursos de ciberseguridad en las carreras de educación superior es indispensable con el fin de enseñar las buenas prácticas a todos los alumnos, pero también para formar profesionales especialistas. La situación nacional es crítica. Se estima que el país tiene un déficit importante de profesionales calificados en ciberseguridad . Esto se explica por varias razones:

1. La inexistencia de una cultura general en ciberseguridad en Chile, y una falta de conciencia de las consecuencias que pueden tener los diversos eventos de ciberseguridad.

2. Una baja oferta de carreras o alternativas de especialización en ciberseguridad en los establecimientos de educación superior en todas las regiones del país.

3. La pobre cultura sobre ciberseguridad no genera una atracción de personas para estudiar temas asociados con la ciberseguridad.

La Academia nacional se encuentra al debe en la implementación de programas formativos, inclusión en sus mallas formativas, y oferta de carreras especializadas en ciberseguridad, si comparamos con la implementación y oferta de carreras técnicas, carreras de ingeniería o de postgrado.

En este contexto, es necesario avanzar con respecto a la oferta educativa superior, por lo cual se desarrollan 4 Propuestas para este ciclo:

Propuesta 8 - Creación de carreras y programas para la formación de especialistas en ciberseguridad

Es necesario aumentar la oferta de profesionales calificados en Chile a través de la creación de carreras y capacitación en el tema.

Acciones a corto plazo

*Crear programas de capacitación profesional en ciberseguridad orientados a profesionales en ejercicio en los rubros de TI y afines.
* Crear capacitaciones en ciberseguridad orientadas a la creación de capacidades ciber en las empresas y las instituciones públicas.
FINANCIAMIENTO: PÚBLICO/PRIVADO

Acciones a mediano plazo

* Crear nuevas carreras en ciberseguridad a varios niveles

* Carreras técnicas de 2 años para formar técnicos superiores en ciberseguridad

* Carreras de pregrado de tipo Ingeniería en Informática o afines con especialidad en ciberseguridad.

* Estudios de post título tipo diplomados y/o Magíster Profesional en ciberseguridad para formar profesionales de alto nivel en el tema.
FINANCIAMIENTO: PÚBLICO/PRIVADO

Acciones a largo plazo

* Generar acuerdos internacionales para el intercambio de alumnos y docentes en carreras de ciberseguridad.
FINANCIAMIENTO: PÚBLICO/PRIVADO

IMPACTOS ESPERADOS

· Aumento de especialistas y profesionales calificados en ciberseguridad en todo el país.

· Mejor formación en ciberseguridad en la educación superior

· Mayor oferta formativa de especialistas.

· Aumento de la experticia nacional en ciberseguridad tanto en las empresas privadas como en las instituciones y organismos del Estado

Propuesta 9 - Incluir nociones de ciberseguridad a todos los niveles de la enseñanza en informática y afines

La ciberseguridad es un tema que actualmente aparece en las carreras de informática como un conjunto de cursos electivos. La consecuencia de este esquema es que los alumnos que no toman estos cursos electivos no tienen nociones básicas de ciberseguridad y de buenas prácticas en el ciberespacio.

Acciones a corto plazo

*Rediseñar los cursos de fundamentos en informática para incluir nociones de ciberseguridad para todos los alumnos, y especialmente en los cursos de:

→Sistemas Operativos.
→Redes de computadores.
→Programación.
→Bases de Datos
→Ingeniería de Software
→Estructuras de Datos.
→Data centers
→Cloud

*Capacitar a los profesores de estos cursos para que tengan el conocimiento de las buenas prácticas en ciberseguridad relacionadas con el tema de sus cursos.
FINANCIAMIENTO: PÚBLICO/PRIVADO

Acciones a mediano plazo

*Implementar los cursos con el nuevo diseño, incluyendo tareas o laboratorios en relación con los aspectos de ciberseguridad relacionados con el tema del curso.
FINANCIAMIENTO: PÚBLICO/PRIVADO

Acciones a largo plazo

* Incluir una formación en ciberseguridad acorde a su especialidad para todas las carreras técnicas y universitarias, equivalentes a lo que hoy son los cursos de matemáticas o ciencias básicas.

* Formar a los docentes de carreras no científicas en las buenas prácticas en ciberseguridad.
FINANCIAMIENTO: PÚBLICO/PRIVADO

IMPACTOS ESPERADOS

· Mejoramiento del nivel general del conocimiento de en ciberseguridad de los alumnos de las carreras de informática y afines, lo que sea la especialidad elegida por los alumnos.

· Aumento general del nivel de conocimientos en ciberseguridad de los alumnos de otras especialidades ajenas a las TI (especialmente en cuanto a las buenas prácticas de uso del ciberespacio).

· Aumento del nivel de conocimientos en ciberseguridad de los profesores de la educación superior en las carreras de informática o afines.

· Aumento del nivel general de conocimientos en cuanto a las buenas prácticas en ciberseguridad de los profesores de la educación superior.

Propuesta 10 - Organizar eventos pedagógicos de ciberseguridad

Es necesario difundir los conocimientos y las buenas prácticas en ciberseguridad, no solamente a través de cursos universitarios, si no que también para un público más amplio, incluyendo aquellas personas interesadas en la ciberseguridad que no posean una formación formal.

Acciones a corto plazo

*Potenciar actividades de difusión durante Octubre, el mes de la Ciberseguridad.

*Organizar talleres de ciberseguridad orientados a alumnos de la educación superior, incluyendo ejercicios de ciberseguridad.

* Organizar eventos de tipo CTF (Capture The Flag) a nivel regional en el país para generar grupos de alumnos Inter universidades expertos en ciberseguridad y detectar talentos regionales en el tema.

Acciones a mediano plazo

*Organizar, durante el mes de la ciberseguridad ejercicios universitarios nacionales (formato CTF u otro) para detectar y generar una red a nivel país de talentos en el tema.

*Organizar talleres de ciberseguridad orientados a empresas (especialmente a las Pymes) para incentivar el uso de las buenas prácticas en ciberseguridad en forma de juegos educativos.

Acciones a largo plazo

*Organizar eventos, ejercicios y competencias de ciberseguridad orientados a las instituciones y organismos tanto públicos como privados

IMPACTOS ESPERADOS

· Detección de talentos en ciberseguridad (a nivel regional y nacional).

· Generación de grupos de entrenamiento a la ciberdefensa.

· Difusión de una cultura de ciberseguridad y de ciberhigiene en las empresas.

Propuesta 11 - Creación de becas temáticas en ciberseguridad de la Agencia Nacional de Investigación y Desarrollo (ANID)

Es necesario crear becas destinadas específicamente a programas de postgrado y proyectos de innovación e investigación aplicada en ciberseguridad.

Acciones a corto plazo

*Creación de becas específicas para postular a programas de postgrado (Magíster Científicos, Magíster Profesionales, Doctorados) en ciberseguridad.

*Creación de becas específicas para pasantías en el extranjero (en países dentro de los 20 primeros en el ranking de la ITU) en temas de ciberseguridad.

*Asignación de Fondos concursables para la academia para proyectos de Ciberseguridad aplicada, que convoquen especialistas locales y extranjeros.

Acciones a mediano plazo

*Creación de financiamientos específicos para proyectos de investigación e innovación en ciberseguridad, especialmente en temas relacionados con la ciberdefensa.

Acciones a largo plazo

*Financiamientos específicos para la creación de centros regionales de innovación e investigación en ciberseguridad con cooperaciones entre la academia y las empresas.

IMPACTOS ESPERADOS

· Financiamientos específicos para la creación de centros regionales de innovación e investigación en ciberseguridad con cooperaciones entre la academia y las empresas.

4.3 EDUCACIÓN CONTINUA

La ciberseguridad es un proceso de carácter continuo, donde constantemente surgen nuevas amenazas y las vulnerabilidades son explotadas con el uso de nuevas herramientas y tecnologías. Las personas y las instituciones se encuentran expuestas a nuevos retos y desafíos que acrecientan la necesidad de una educación continua y permanente, que vaya instruyendo sobre nuevos retos, nuevas herramientas y soluciones en la ciberseguridad, y de la cual debemos hacernos cargo.

En consecuencia, se indican las siguientes 4 propuestas para abordar este aspecto.

Propuesta 12 - Generación de Diplomas y Certificaciones de Competencia

Fomentar la generación de Diplomas y Certificaciones acorde con las necesidades del ecosistema chileno.

Acciones a corto plazo

*Generar planes de programas de certificación amplios que recojan las necesidades de instituciones tanto públicas como privadas.
FINANCIAMIENTO: PÚBLICO

Acciones a mediano plazo

*Fomentar la homologación de certificaciones nacionales a estándares internacionales que puedan ser otorgadas por las instituciones de formación nacional, con las acreditaciones correspondientes.
FINANCIAMIENTO: PÚBLICO / PRIVADO

Acciones a largo plazo

*Establecer certificaciones que permitan acreditar una competencia básica en Ciberseguridad (ej: similar al Carné de Conducir), tendientes a incentivar carreras profesionales en Ciberseguridad en línea con las Certificaciones en Ciberseguridad Internacionales.
FINANCIAMIENTO: PÚBLICO

IMPACTOS ESPERADOS

· Fomentar, actualizar y homologar la certificación a nivel internacional en materia de ciberseguridad a los funcionarios de las distintas instituciones (Públicas y privadas) para reducir las brechas detectadas.

· Fomentar la capacitación del personal institucional en las certificaciones internacionales en Ciberseguridad definidas en los programas de certificación homologados para el país en las instituciones formativas (público / privadas) certificadas.

· Convertir al país en referente en ciberseguridad al generar un Certificado nacional básico (abierto a toda la población) para que se dominen tópicos básicos y dar continuidad de estudio homologado con los más altos estándares internacionales.

Propuesta 13 - Capacitación de empresas y organismos estatales

Mejorar el nivel general de capacitación en ciberseguridad del personal de las empresas y de los organismos estatales. Tratar la ausencia de un diagnóstico del estado de madurez en ciberseguridad. Exponer un modelo único y nacional para desarrollar el análisis de madurez.

Acciones a corto plazo

* Realizar un catastro y diagnóstico en distintas Instituciones del nivel de ciberseguridad. Asimismo, determinar si existe personal competente o especializado para operar en la materia.
FINANCIAMIENTO: PÚBLICO / PRIVADO

Acciones a mediano plazo

*El Estado deberá patrocinar iniciativas e incentivos, promoviendo vínculos con otras instituciones (internacionales o nacionales) públicas y privadas, para acortar las brechas diagnosticadas, con el propósito de generar planes directores en capacitación sectoriales para poder cubrir las brechas.
FINANCIAMIENTO: PÚBLICO

Acciones a largo plazo

*Consolidar el ecosistema (Públicas y privadas) como promotor de mejora continua en materias de educación de ciberseguridad con foco para empresas y organismos estatales.
FINANCIAMIENTO: PÚBLICO/PRIVADO

IMPACTOS ESPERADOS

· Tener un catastro actualizado de las fortalezas y deficiencias de los funcionarios públicos en las distintas instituciones. Determinar qué tan vulnerables son nuestras instituciones y si existen sistemas de seguridad en ellas. Determinar el nivel de madurez (capacitación) de las mismas. Objetivo operacional tecnológico.

· Disminución de las brechas detectadas en el diagnóstico, fomentando un ecosistema de mejora continua.

· Consolidación del ecosistema (Públicas y privadas) como promotor de mejora continua en materias de educación de ciberseguridad con foco para empresas y organismos estatales.

Propuesta 14 - Sensibilización de los ciudadanos

Educar a las personas acerca de la ciberseguridad es de vital importancia para la creación de una cultura nacional en la materia. La conciencia es el primer paso hacia el desarrollo de una ciudadanía con buenas prácticas de ciberhigiene Generar campañas de sensibilización permanentes, tendientes a educar a los ciudadanos según sus propias necesidades, reforzando la creación de una cultura nacional en ciberseguridad.

Acciones a corto plazo

***** CREACIÓN DE UN LEMA Y MARCA. El lema es esa frase corta, concisa, que será fácilmente reconocible y establecerá el tono de la campaña. Juntos, el lema y el logotipo son el mensaje breve y la imagen gráfica que les anuncia a todos *"presten atención, aquí hay algo en lo que ustedes deben conocer y que deben aplicar"*. Estos dos elementos constituyen los elementos de marca de la campaña.

→Desarrollar una idea fuerza que se consagre en un texto y una imagen (un logo), destinados a resaltar los beneficios de la ciberseguridad (similar a la campaña Elige Vivir Sano del Ministerio de Salud).

→Establecer un programa masivo de difusión de esa idea fuerza. Utilización en todos los portales gubernamentales. Colocar el logo y uno o dos consejos de campaña en un banner o ventana emergente en todos los portales o Sitios web a los que accede el público.

FINANCIAMIENTO: PÚBLICO

Acciones a mediano plazo

***** Creación y difusión de herramientas de seguridad cibernética para empresas.

→Hoja informativa para trabajadores que contenga los mensajes que les corresponde por área del negocio. (Asimilable al "Derecho a Saber" en la legislación laboral)

→Una lista de medidas fáciles de implementar para mejorar de inmediato su situación en seguridad digital. (asimilable a los EPP: elementos de protección personal)

→Carteles para el lugar de trabajo. (señalética de ciberseguridad)

FINANCIAMIENTO: PÚBLICO/PRIVADO

Acciones a largo plazo

***** Creación de una Oficina Virtual de asesoría en ciberseguridad para el Internauta (que incluya atención telefónica).
FINANCIAMIENTO: PÚBLICO/PRIVADO

IMPACTOS ESPERADOS

· El mensaje y el logo proporcionan la identidad del programa

· Sensibilizar a los empresarios, trabajadores y comunidad en general.

· Proporcionar información y soporte al usuario final para resolver inquietudes y problemas de seguridad que le pueden surgir al navegar por Internet, sobre todo en sus primeros pasos en las nuevas tecnologías.

Propuesta 15 - Formación y acompañamiento a Adultos Mayores

Exponer los diferentes conceptos asociados a problemáticas que sufre el adulto mayor en un mundo digital; Mostrar las medidas que se han tomado hoy en día a nivel nacional, internacional y analizar experiencias comparando resultados y proponer nuevas soluciones.

Acciones a corto plazo

*Identificar Instituciones/Organizaciones con las que se pueda alcanzar al público objetivo (Adulto Mayor).
FINANCIAMIENTO: PÚBLICO / PRIVADO

Acciones a mediano plazo

* Realización de talleres prácticos; cursos básicos de informática, cuidados básicos en ciberseguridad, presenciales y online (dependiendo del nivel), a usuarios de redes SENAMA.
FINANCIAMIENTO: PÚBLICO

Acciones a largo plazo

* Creación de herramientas de acompañamiento (Fonos de contacto, WhatsApp, Aplicaciones, Test online) que permitan al adulto mayor informarse y apoyarse para navegar seguro.
FINANCIAMIENTO: PÚBLICO/PRIVADO

IMPACTOS ESPERADOS

· Formar en los siguientes aspectos mínimos, incentivando una política de facilitadores entre pares :

→Administración Electrónica 1: Operación sistema clave única y en servicios públicos.
→Administración Electrónica 2 y Banca on-line: operaciones y cuidados en sistemas de pagos electrónicos y banca.

→Comunicación digital. Herramientas de comunicación, correo electrónico, WhatsApp y Videoconferencias.
→Manejo de Móviles: Usos más habituales.
→Aplicaciones para Móviles: Aplicaciones más usadas.

· Formar una red de asistencia al Adulto mayor.

4.4 TEMAS TRANSVERSALES

Como se señaló anteriormente, consideramos necesario incluir algunas propuestas complementarias que sirven para el desarrollo de talento ciber, y que deben ser consideradas en su justo mérito para fomentar la cultura y el desarrollo de la ciberseguridad nacional.

Esto se refleja en las siguientes 4 propuestas:

Propuesta 16 - Generar la "Plataforma nacional de Ciber formación y ciber empleos– orientado a Ciberseguridad"

Ausencia de nexos eficientes para la reconversión. Exponer métodos para fomentar la reconversión.

Acciones a corto plazo

* Realizar un estudio en conjunto con la academia y organizaciones de la sociedad, para estimar demandas y público objetivo.
FINANCIAMIENTO: PÚBLICO / PRIVADO

Acciones a mediano plazo

* El Estado patrocinará iniciativas e incentivos, a través de organismos como Sence, al objeto de establecer una bolsa nacional de empleos tecnológicos, digitales y de ciberseguridad. A lo anterior se promoverá un programa nacional de reconversión profesional a ciberseguridad. (base Corfo: Becas Capital Humano)
FINANCIAMIENTO: PÚBLICO

Acciones a largo plazo

*Generar ferias laborales con foco en reconversión laboral, de personal en retiro de fuerzas armadas, empleados públicos, mujeres y ciudadanos neuro diverso similar a como se realiza en EE. UU.
FINANCIAMIENTO: PÚBLICO/PRIVADO

IMPACTOS ESPERADOS

· Tener un estudio a nivel nacional de sectores y profesiones que podrían ser parte de un programa de educación con foco en reconversión.

· Aumentar la reconversión profesional a especialistas en ciberseguridad.

· Generar un sistema de capital humano para fortalecer la demanda de especialistas en Chile. .

Propuesta 17 - Creación del Instituto Nacional de Ciberseguridad **(INCIBER)**

Es necesario crear un Instituto Nacional de Ciberseguridad en Chile, como es el caso de España (con el INCIBE). El rol del INCIBER chileno será la creación de un ecosistema de ciberseguridad, cubriendo la difusión, innovación y fomento de la ciberseguridad, incluyendo el mundo académico, el mundo empresarial, los organismos del Estado y la sociedad civil organizada.

Acciones a corto plazo

*Creación de normas nacionales de referencia para la educación de los futuros expertos en ciberseguridad en el país. Cumplir un rol articulador en la investigación y desarrollo nacional de la ciberseguridad. Establecer nexos con instituciones afines a nivel internacional.
FINANCIAMIENTO: PÚBLICO

Acciones a mediano plazo

*Organizar ejercicios nacionales de ciberseguridad en conjunto con la academia para fomentar el aprendizaje en grupo de técnicas de ciberdefensa, así como detectar talentos en la materia.
FINANCIAMIENTO: PÚBLICO

Acciones a largo plazo

* Generar certificaciones nacionales en ciberseguridad (al estilo del EC-Council) en cooperación con los establecimientos de educación superior.

* Generar un sistema de acreditación en ciberseguridad para cursos sobre la materia (un *label* de calidad: Sello INCIBER)
FINANCIAMIENTO: PÚBLICO/PRIVADO

IMPACTOS ESPERADOS

· Creación de un ecosistema entre el Estado, la academia y las empresas para generar un marco de cooperación en educación y difusión en ciberseguridad.

· Creación de un modelo de certificación de la educación en ciberseguridad.

· Mejora de la cooperación entre el mundo académico y el mundo empresarial en ciberseguridad.

Propuesta 18 - Crear un equivalente de la *Estonian Defence League's Cyber Unit* de Estonia

La Estonian Defence League's Cyber Unit es una organización que tiene como objetivo la defensa del ciberespacio del país. Incluye miembros de organizaciones estatales especialistas en ciberseguridad, así como profesionales de empresas privadas y voluntarios de la sociedad civil.

Acciones a corto plazo

* Creación de una asociación para la defensa del ciberespacio chileno en cooperación con el mundo académico, representantes del Estado, profesionales en ciberseguridad y voluntarios de la sociedad civil.
FINANCIAMIENTO: PÚBLICO

Acciones a mediano plazo

* Crear una división en el INCIBER para la gestión, la implementación y el entrenamiento de esta asociación.
FINANCIAMIENTO: PÚBLICO/PRIVADO

Acciones a largo plazo

* Organizar ejercicios de entrenamiento a nivel internacional para los miembros de esta asociación de defensa del ciberespacio chileno (por ejemplo, en cooperación con Estonia u otros países de buen ranking en ciberseguridad).
FINANCIAMIENTO: PÚBLICO/PRIVADO

IMPACTOS ESPERADOS

· Tener una reserva nacional de especialistas en ciberseguridad para poder enfrentar cualquier escenario de ataque a nivel nacional.

· Generar una cooperación entre el mundo civil y militar en ciberseguridad (Ministerio de Defensa y Ministerio a cargo de la Seguridad Pública).

· Detectar y promover a talentos en ciberseguridad que no están en el sistema tradicional de educación superior.

Propuesta 19 - Generar una cultura de cuidado de datos personales en la ciudadanía

La protección de los datos personales es ahora fundamental para proteger a los jóvenes de ataques de tipo cyberbullying, pero también para asegurar la 'privacidad de las personas en general. El cuidado de los datos personales debe ser parte de una cultura nacional en el tema y de los talentos digitales de cada uno.

Acciones a corto plazo

* Generar campañas de sensibilización sobre el cuidado e importancia de los datos personales en los medios de comunicación
FINANCIAMIENTO: PÚBLICO

Acciones a mediano plazo

* Avanzar en la promulgación de la ley de protección de datos personales, basado en el RGPD Reglamento General de Protección de Datos europeo.

* Establecer una identidad digital nacional robusta con doble autenticación.
FINANCIAMIENTO: PÚBLICO

Acciones a largo plazo

* Restringir el uso del RUT como identificación, sujeto al consentimiento previo entre las partes respecto del uso y destino de la información entregada, y existencia de una identidad digital robusta.
FINANCIAMIENTO: PÚBLICO

CONCLUSIONES

Para que Chile avance en ciberseguridad, es necesario hacer un gran esfuerzo en la educación y especialmente en la formación de profesionales altamente calificados en el tema. Para eso, la creación de un ecosistema completo de ciberseguridad a nivel del país es indispensable para poder adecuar la oferta académica a las necesidades de nuestro país.

Sin embargo, es necesario tomar en cuenta la educación temprana en ciberseguridad para asegurar una preparación adecuada de los niños y niñas a en el uso de Internet en general. La educación temprana es la mejor forma de construir una cultura nacional en ciberseguridad, generando las bases para una ciberhigiene de alto nivel en todas las capas de la población chilena.

Por otro lado, la ciberseguridad es una parte muy dinámica de la informática, y con constantes cambios. Eso implica que la formación continua en ciberseguridad en fundamental para mantener un alto nivel de preparación, tanto en las empresas privadas como en los organismos del Estado. De este punto de vista, la oferta, en términos de estudios de postgrado y especialmente de los diplomas y diplomados en ciberseguridad, debe hacerse de acuerdo con las necesidades de las empresas y con miras a resguardar al país y a sus ciudadanos.

*Capítulo 3_*

Investigación Avanzada en Ciberseguridad (IAC)

PARTICIPARON EN LA ELABORACIÓN DE ESTE TEXTO:

- Equipo Coordinador submesa "Investigación Avanzada en Ciberseguridad": Romina Torres y Pedro Pablo Pinacho

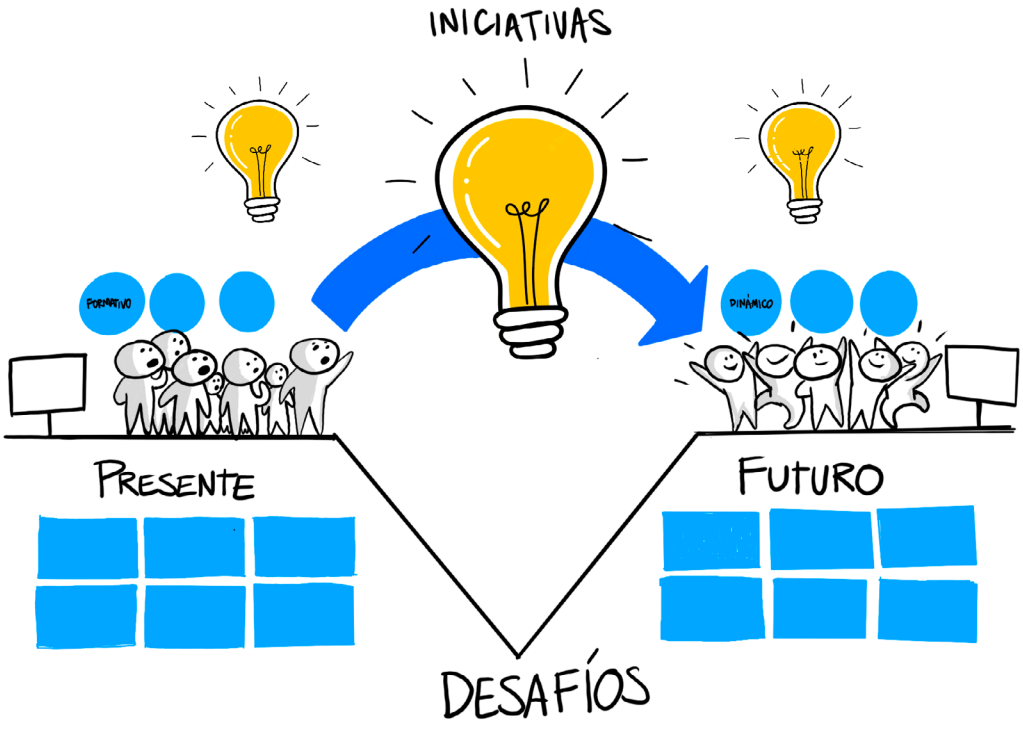
- Comité de Trabajo Técnico de la submesa "Investigación Avanzada en Ciberseguridad" convocado por la Comisión formado por: Andrés Barrientos, Mauricio Romo, Jorge Flores, Ricardo Monreal, Claudio Galleguillos Escobar, Danic Maldonado, Rodrigo Bustamante, Claudia Negri, Francisco García, Sergio Leiva, Carlos Manzano, Julio López Fenner, Ricardo Seguel, Rocío Ortiz, Alejandro Hevia, Gonzalo Díaz de Valdés, Javier Ramírez y Amalia Pizarro Madariaga

1. INTRODUCCIÓN

En 10 reuniones de trabajo/dinámicas, desarrolladas entre el 16 de Julio y el 26 de octubre de 2022, un equipo conformado por 8 profesionales cada reunión en promedio de formaciones diversas entre los que se cuentan ingenieros, empresarios, académicos y militares, lograron el resultado que se refleja en este capítulo.

El propósito ha sido analizar el estado actual de la investigación en ciberseguridad, y desde esa base proponer una estrategia público privada para enfrentar la investigación avanzada donde la academia cumple el rol articulador por excelencia .

Este capítulo entrega una Lista de Iniciativas Priorizadas en materia de investigación en ciberseguridad que aseguren, a quienes aspiren a realizar investigación avanzada en ciberseguridad en Chile, el acceso a infraestructura, a recursos, a espacios que visibilicen sus resultados y transferencia tecnológica que permitan posicionar al país gradualmente como actor relevante a nivel internacional al 2035 por medio del aumento gradual en el nivel de madurez en I+D en ciberseguridad (acorde al modelo de la Universidad de Oxford) al corto plazo a "establecido" (4 años), al mediano a "estratégico" (8 años) y al largo plazo a "dinámico"(12 años).



2. CONTEXTO

Modelos de referencia para evaluar la madurez de los países en la arista investigación

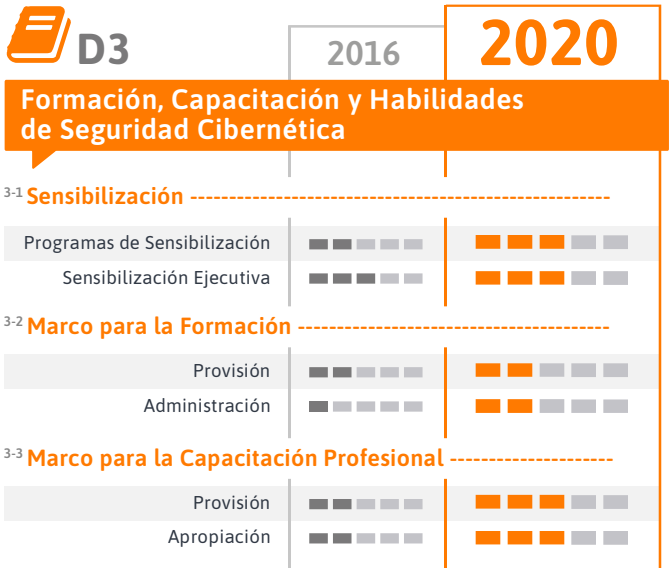
Se ha considerado relevante conocer los modelos que permiten determinar el grado de madurez de los países en materia de investigación en Ciberseguridad, de manera de poder establecer una hoja de ruta desde un nivel base acorde a la realidad nacional.

Modelo de Madurez de Ciberseguridad para las Naciones (CMM)

El Modelo de Madurez de Ciberseguridad para las Naciones es propuesto por el Centro de Ciberseguridad Global de la Universidad de Oxford. Este modelo ha sido aplicado para evaluar a Chile en 2016 y 2020. El modelo se divide en dimensiones y factores, donde ambos pueden ser evaluados en cinco niveles de madurez: "1-inicial", "2-formativo", "3-establecido", "4-estratégico" o "5-dinámico".

Fuente: https://gcscc.ox.ac.uk/dimension-3-cybersecurity-knowledge-and-capabilities

La Dimensión 3 de este modelo se centra en Educación, Capacitación y Habilidades en Ciberseguridad donde el Factor D3.4: Investigación e Innovación en Ciberseguridad aborda la madurez en las capacidades de investigación en las naciones. Ahora bien, este factor fue agregado en la versión publicada en 2021. Por lo que las capacidades en materia de investigación avanzada en Chile no han sido evaluadas por este modelo. Ahora bien, en la Imagen siguiente es posible ver que Chile fue en materias de marco para la formación de nuevos profesionales se encuentra en un nivel 2 de madurez y en materias de sensibilización y capacitación profesional ha aumentado de 2 a 3.



Fuente: Ciberserguridad Riesgos, Avances y el Camino a seguir en America Latina y el Caribe. Reporte Ciberseguridad 2020 BID-OEA

Se estima que en el factor 3.4, el País presenta un nivel entre inicial a formativo pues existen **actividades I+D limitadas en ciberseguridad** en el País pues se cuenta con algunas redes de investigación colaborativa intra-país (entre organismos academia/empresas y policías o fuerzas armadas) y otras más incipientes inter países. Esta estimación es resultado de la aplicación de los criterios del factor en el aspecto Investigación y Desarrollo:

Factor - D 3.4: Cybersecurity Research and Innovation

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

Fuente: Cybersecurity Capacity Maturity Model for Nations (CMM) - 2021

1. NIVEL INICIAL

- si no tiene o tiene actividades I+D limitadas en ciberseguridad en el País.

2. NIVEL FORMATIVO

- si estas actividades ocurren en red al menos dentro del País o con un País socio que entienda cómo se aplica la investigación y el desarrollo al contexto local del País.
- si el País participa incipientemente en redes de investigación colaborativas regionales/internacionales en ciberseguridad.
- si existen métricas de rendimiento en I+D en ciberseguridad, pero aún son limitadas en alcance o ad-hoc.

3. NIVEL ESTABLECIDO:

- si las actividades de I+D en ciberseguridad han sido establecidas y son indicadas en la estrategia nacional de ciberseguridad.
- si los recursos y procesos requeridos para entregar las acciones de las actividades de I+D en ciberseguridad han sido identificadas y están en funcionamiento.
- si el Financiamiento es el adecuado para realizar estas actividades.
- si existe una colaboración regional/internacional activa con prácticas y desarrollos.
- si el País está activamente participando y contribuyendo a las redes de colaboración regional/internacional.
- si las métricas para medir el rendimiento de la I+D están funcionando y permiten medir el progreso y mejorar las capacidades de I+D en el País.

4. NIVEL ESTRATÉGICO

- si el país está activamente construyendo comunidades de interés alrededor de las prioridades I+D en ciberseguridad
- si la estrategia I+D está en funcionamiento completamente
- si el país hace una mayor contribución a la I+D en ciberseguridad y está activamente involucrado en construir capacidades de innovación en esta industria a través de consorcios internacionales de I+D e inversión.
- si los riesgos emergentes en ciberseguridad son regularmente medidos y usados para actualizar la estrategia nacional y el desarrollo futuro de los programas de la estrategia de I+D

5. DINÁMICO

- si el país es el actor líder en investigación e innovación y está en los debates internacionales en el desarrollo de los planes estratégicos de I+D en ciberseguridad.
- si el País está mirando hacia el futuro, viendo los problemas emergentes alrededor de nuevos tipos de tecnología o amenaza, y usa la I+D para preparar un ambiente futuro para amenazas.
- si el País está contribuyendo a las mejores prácticas en I+D en ciberseguridad

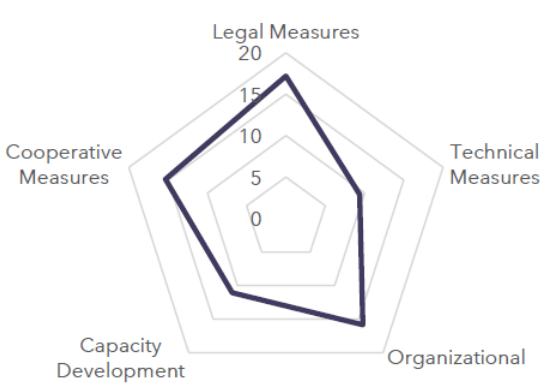
Cyber Security Index (CGI)

Otro modelo es el de la **Organización Internacional de Telecomunicaciones (ITU)** que permite establecer una situación base. En particular, el Pilar #4 busca la "Generación de capacidades: la evaluación de medidas adoptadas para la generación **capacidades y competencias** (investigación y capacitación), así como procesos de certificación de profesionales (certificaciones, capacitaciones, investigación, generación de industria y servicios, campañas de prevención, entre otros), apuntado a contar con un cuerpo de expertos y profesionales en la materia".

En ese sentido, es interesante observar los indicadores que usan para poder medir la inversión en programas nacionales de investigación y desarrollo en ciberseguridad en instituciones, que pueden ser privadas, públicas, académicas, no gubernamentales o internacionales.

Considera la presencia de un organismo institucional reconocido a nivel nacional que supervise el programa. Los programas de investigación de ciberseguridad incluyen, entre otros, análisis de malware, investigación de criptografía e investigación de vulnerabilidades del sistema y modelos y conceptos de seguridad. Los programas de desarrollo de ciberseguridad se refieren al desarrollo de soluciones de hardware o software que incluyen, entre otros, firewalls, sistemas de prevención de intrusiones, honeypots y módulos de seguridad de hardware. La presencia de un organismo nacional general aumentará la coordinación entre las diversas instituciones y el intercambio de recursos.

Chile



Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
68.83	17.20	9.39	15.84	11.07	15.33

Source: ITU Global Cybersecurity Index v4, 2020

Acorde a los Informes de la ITU, para mostrar evidencia de que un País está maduro en materias de investigación avanzada debe existir evidencia clara de lo siguiente:

- **Actividades de I+D** en ciberseguridad a nivel nacional
- **Programas de I+D** en ciberseguridad en el **sector privado**
- **Programas de I+D** en ciberseguridad en el **sector público**
- Participación en **actividades de I+D de las instituciones de educación superior**, como la academia y las universidades
- Existencia de **mecanismo de incentivo gubernamental** en el lugar. Por ejemplo, a través de exenciones fiscales, subvenciones, financiación, préstamos, disposición de instalaciones y otros motivadores económicos y financieros, incluidos los motivadores institucionales dedicados y reconocidos a nivel nacional.
- Existencia de un **organismo que supervisa las actividades de desarrollo de capacidades en ciberseguridad.** Los incentivos aumentan la demanda de servicios y productos relacionados con la ciberseguridad, lo que mejora las defensas contra las ciberamenazas.
- **Mecanismos de fomento para el desarrollo de capacidades para el desarrollo de una industria de ciberseguridad**

ENISA

ENISA (European Union Agency for Cybersecurity) publicó en septiembre del 2022 el marco de trabajo para definir las habilidades necesarias para los diferentes perfiles tanto para la investigación como para otras habilidades. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

Declara que **"Un investigador en Ciberseguridad es aquel que investiga en materias de ciberseguridad e incorpora estos resultados en soluciones de ciberseguridad"**. Conduce investigación aplicada y básica/fundamental, coopera con stakeholders, conduce experimentos y desarrolla prueba de conceptos, pilotos y prototipos para soluciones en ciberseguridad, conoce estándares, metodologías y marcos de trabajo en ciberseguridad, además de requerimientos legales y regulatorios como también procedimientos de seguridad de la información.

Un investigador en Ciberseguridad posee mostrar evidencia de conocimientos, competencias y habilidades:

Conocimientos

- investigación, desarrollo e innovación en ciberseguridad

- estándares, metodologías y marcos de trabajo en materia de ciberseguridad

- requerimientos legales, regulatorios y legislativos en liberar o usar tecnologías de ciberseguridad

- aspectos multidisciplinariot en ciberseguridad

- procedimientos de no revelación de información

Competencias

- monitoreo de tendencias en tecnología

- innovador

- analítica y ciencia de datos

- gestión de problemas

- gestión de información y conocimiento

Habilidades

- genera nuevas ideas y transfiere teoría a práctica

- descompone y analiza sistemas para identificar debilidades y controles inefectivos

- descompone y analiza sistemas para desarrollar soluciones que aborden los requerimientos de seguridad y privacidad

- monitorea nuevos avances en tecnologías relacionadas a ciberseguridad

- comunica, presenta y reporta a los stakeholders relevantes

- identifica y resuelve problemas de ciberseguridad

- colabora con otros miembros de equipo y colegas

Las tareas que debe realizar un Investigador en ciberseguridad son:

- analizar y evaluar las tecnologías, soluciones, desarrollos y procesos de ciberseguridad

- conducir investigación, innovación y desarrollo en tópicos asociados a la ciberseguridad

- Manifestar y generar ideas innovadoras

- Aportar con avances al estado del arte

- Asistir en el desarrollo de soluciones innovadoras en ciberseguridad

- Conducir experimentos y desarrolla prueba de conceptos, pilotos y prototipos para soluciones en ciberseguridad

- Contribuir con servicios, soluciones y productos de ciberseguridad innovadores

- Asistir en la construcción de capacidades asociadas a ciberseguridad tales como concientización, entrenamiento técnico y práctico, mentoría, testing, supervisión

- Identificar avances en materia de ciberseguridad y aplicarlos en sus enfoques y soluciones

- liderar o participar en los procesos de innovación

- publicar y presentar trabajos científicos y resultados de I+D

3. SITUACIÓN BASE DEL PAÍS EN IAC

En nuestra Política Nacional de Ciberseguridad 2018-2022 (PNC) señala como objetivo E de la misma, siguiente: " El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus Objetivos Estratégicos (OE), donde se destaca:

OE-PNC1 [Relevar] Importancia de la innovación y desarrollo en materia de ciberseguridad

OE-PNC2 [Posicionar] Ciberseguridad como medio para contribuir al desarrollo digital de Chile

OE-PNC3 [Posibilitar] Desarrollo de la industria de ciberseguridad en Chile

OE-PNC4 Contribuir a la generación de oferta por parte de la industria local

OE-PNC5 [Estimular] Generación de demanda de parte del sector público basado en los intereses estratégicos del Estado

Y la Medida 41- **OE-PNC6** Incentivar la exportación de productos y servicios nacionales en el área de ciberseguridad, identificando ferias internacionales y evaluando fuentes de apoyo.

Si dicha política hubiese alcanzado los objetivos y medida anteriormente mencionados, entonces sería esperable que el País en materias de IAC tuviese un mejor nivel de madurez en el factor 3.4 de la dimensión 3 del CMM.

En efecto, de existir una Industria de ciberseguridad nacional que diese importancia a la innovación en materia de ciberseguridad, sus productos ya estarían en operación al menos satisfaciendo oferta local, contribuyendo al desarrollo digital de Chile desde la perspectiva "segura", e incipientemente estaría iniciando la exportación de estos productos a nivel internacional. Por tanto, probablemente estaría **participando** activamente en **foros y discusiones internacionales como referente.**

Sólo analizando la política y su operacionalización actual acorde a lo indicado por los modelos de referencia de evaluación, se detectan las siguientes brechas (B) o necesidades:

B1 Falta de referencia a una Política Internacional en materias de ciberseguridad

B2 Falta de participación del País en instancias multilaterales y globales apoyando de la misma forma procesos de consulta regional, subregional y multilateral en el área, particularmente en América Latina (al menos en materia de I+D en ciberseguridad).

B3 Falta de alianzas importantes entre organismos de seguridad interior y defensa exterior con la industria nacional en el área.

B4 Falta de aprovechamiento de la oportunidad que se tiene de hacer crecer el Sector TIC (representaba el 2017 cerca de un 3-4,12% del total de la economía chilena, en los países OECD este sector promediaba un 6% de participación en la economía de los países) mediante el desarrollo del componente de ciberseguridad dentro de esa industria.

B5 Falta de identificación de los dominios estratégicos para desarrollar en el corto, mediano y largo plazo. Ejemplo: industria nacional vinculada al desarrollo y uso de estándares de cifrado.

B5.1 Falta de identificación de oferta de productos resultantes de procesos I+D en materias de ciberseguridad por parte de la industria local.

B5.2 Falta de identificación de la Demanda de parte del sector público que debería atender la Industria de Ciberseguridad.

B6 Nivel de Madurez insuficiente en la dimensión de I+D en Ciberseguridad.

Medidas específicas en Políticas Nacionales de ciberseguridad que fueron declaradas para ser ejecutadas durante el periodo 2017-2018, pero no es posible evidenciar resultados por lo que son descritas en este documento como brechas:

B-MINSEGPRES – Ausencia de una norma técnica para el desarrollo o contratación de software en el Estado, acorde a estándares de desarrollo seguro.

B-MINREL-1 – Inexistencia o desconocimiento de un grupo de trabajo interagencial para abordar temas internacionales relativos al ciberespacio.

B-MINREL-2 Intercambio insuficiente de experiencias con otros países en materia de ciberseguridad (Benchmarking)

B- CORFO - MINDEF - MINECON – Ausencia o número insuficiente de programas especiales para impulsar la industria de ciberseguridad nacional, en sectores definidos.

B-MINREL (Prochile) - MINECON - Instrumentos de fomento y apoyo insuficientes para la exportación de productos y servicios nacionales en el área de ciberseguridad

Por otro lado, también se evidencian las siguientes debilidades para realizar IAC en Chile:

· Falta de Infraestructura para desarrollar investigación en ciberseguridad

· Falta de demanda de capacidades de investigación en ciberseguridad a nivel País (más cuando se considera la interdisciplinariedad)

· Falta de visibilidad de los resultados de las iniciativas de investigación existentes

· Falta Industria en Ciberseguridad de base científica tecnológica

· Falta de Presupuesto Nacional para desarrollar actividades de investigación en materia de ciberseguridad

4. SITUACIÓN FUTURA

La IAC debe asegurar a los investigadores el acceso a infraestructura, a recursos, a espacios de visibilización de sus resultados y transferencia tecnológica que permitan posicionar al país al 2035 en el cuadrante de líderes en la industria I+D en ciberseguridad.

Tomando el CMM como un modelo a considerar, nuestro desarrollo debe tender a permitir alcanzar en I+D en ciberseguridad a corto plazo un nivel "3-establecido", a mediano plazo un nivel "4-estratégico" y a largo plazo un nivel "5-dinámico".

Para ello se considera relevante desarrollar una Estrategia Nacional en Ciberseguridad, con su correspondiente plan operativo de IAC que explícitamente señale y considere:

Para el corto plazo (4 años), tendiente a obtener el nivel de madurez **"3-Establecido":**

1. Las actividades de IAC que se realizan en el País,

2. Los recursos y procesos requeridos para realizar las actividades de IAC,

3. Las fuentes de financiamiento adecuadas para realizar estas actividades,

4. Los actores regionales e internacionales con los que se realiza investigación además de mostrar evidencia de redes de colaboración regional/internacional con prácticas y desarrollos,

5. Las métricas y sus valores que permiten medir el rendimiento de las acciones de IAC y cómo se ha progresado.

Para el mediano plazo (8 años) , y consolidado el nivel de establecido, para alcanzar un nivel de madurez **"4-Estratégico"**:

1. Las comunidades alrededor de las áreas prioritarias de IAC

2. Evidencia de que el apartado en I+D de la Estrategia Nacional en Ciberseguridad está funcionando completamente

3. Los aportes de financiamiento para contribuir a la I+D en ciberseguridad

4. Los consorcios internacionales de I+D e inversión para construir capacidades de innovación en materias de IAC.

5. los riesgos emergentes en ciberseguridad que están siendo abordados, mostrando evidencia de que son regularmente medidos y usados para actualizar la estrategia nacional y en particular el apartado de programas de IAC.

Finalmente, y para el largo plazo (12 años) para alcanzar un nivel de madurez "5-Dinámico", deben existir evidencias:

1. en los rankings relevantes de que Chile está en el cuadrante de líder en investigación e innovación en ciberseguridad.

2. de los debates internacionales en los que Chile está aportando en el desarrollo de los planes estratégicos regionales de I+D en ciberseguridad.

3. de una unidad de observación que identifique los problemas emergentes alrededor de nuevos tipos de tecnología o amenaza

4. de actividades I+D para prepararse a amenazas futuras.

5. de generación de las mejores prácticas en I+D en ciberseguridad.

5. PROGRAMA DE INICIATIVAS PRIORITARIAS

Con el fin de ir avanzando hacia la situación futura deseada en los términos señalados en el punto anterior se proponen los siguientes programas de acción:

Programa 1: Centro Nacional de Investigación en Ciberseguridad

Pilar: Capacidades de Investigación

Objetivo: Consolidar en Chile un centro de desarrollo de capacidades cibernéticas que sea referente en la región en investigación avanzada en materias de ciberseguridad en sus diversas áreas de especialización.

Descripción: Busca tener equipos de investigadores colaborando para abordar desafíos y amenazas prioritarias para el País, que permita unir a nuevos investigadores en diferentes niveles por reducir las brechas de entrada o reconvertir otros de áreas afines.

Acciones previas:

· Levantar

→ Plataforma para realizar Catastro nacional de investigadores en ciberseguridad

→ Catálogo indexado sobre github de las publicaciones (papers/tesis/ reportes, códigos y datasets) que se están generando en Chile

→ Catastros de Centros de investigación colaborativa intersectorial alrededor de la ciberseguridad

→ Levantar Catastro de Redes de Investigación Colaborativas para Ciberseguridad intra-país, inter-organismos, a nivel regional e internacional.

· Generar

→ Reporte Anual de Estudio de áreas prioritarias relevantes actuales, emergentes y futuras en Ciberseguridad susceptibles de ser abordadas

→ Dashboard de métricas asociadas a IAC en Chile

→ Dashboard Web Anual de amenazas futuras y riesgos emergentes en ciberseguridad

Acciones

· Generar Comunidades de IAC en:

→ Machine Learning Poisoning
→ Optimización de capacidades de detección
→ Criptografía
→ Interoperabilidad
→ Identidad digital con biometría
→ Fake News y Desinformación en línea
→ Resiliencia en infraestructura Crítica/IoT
→ Investigación Forense Digital
→ Ciudades Inteligentes y subcomunidades (e.g. Smart Health)
→ regulaciones, legislación.
→ Ciberseguro por diseño
→ Privacidad por diseño
→ Investigación en ciberseguridad

Métricas

· Número de:

→ Áreas de trabajo en IAC

→ Riesgos emergentes en ciberseguridad del año anterior, actual o futuro reconocida como prioritaria para el País
→ Iniciativas generando IAC en amenazas futuras
→ Publicaciones Scopus/Wos
→ Datasets liberados
→ Herramientas liberadas
→ Capacitaciones
→ Instancias de divulgación realizadas
→ Citas a publicaciones
→ Proyectos en los que participa la comunidad financiados por ANID (Agencia Nacional de Investigación y Desarrollo)
→ Proyectos o en colaboración con organismos públicos y organismos privados
→ Proyectos en colaboración internacional
→ Aportes en catálogo por tipo
→ Doctores en IAC insertos en Industria

· Porcentajes de:

→ Amenazas abordadas
→ Riesgos emergentes abordados
→ Doctores en IAC insertos en Industria
→ Comunidades activas
→ Investigadores reconocidos actualizando información en plataforma anualmente
→ Uso del catálogo indexado

· Tasa de investigadores y aporte a catálogo indexado

Programa 2: Centro de escalamiento y nuevos negocios en torno a resultados de investigación en ciberseguridad

Pilar: Capacidades de Innovación, Desarrollo Tecnológico aplicado y Negocios

Objetivo: Facilitar el desarrollo de la industria de productos y servicios de base científica-tecnológica en el área de ciberseguridad en Chile que ayude a posicionar al País en innovación, la investigación aplicada y el desarrollo tecnológico en ciberseguridad

Descripción: Busca unir investigadores del país trabajando actualmente en silos en torno a proyectos colaborativos nacional/internacionalmente además de multidisciplinarios y que consideran Instituciones del Estado, de Defensa, en general públicos y privados, de manera de incubar y escalar desarrollos de base científico tecnológico al mercado nacional como internacional. entrada o reconvertir otros de áreas afines.

Acciones previas:

· Generar Estudio de caracterización de Industria
· Generar Alianzas importantes entre organismos de seguridad interior y defensa exterior con la industria nacional en el área.
· Levantar Plataforma de desafíos de IAC de manera interdisciplinaria
· Impulsar un Desafío de Innovación Pública (iniciativa conjunta entre ANID y Laboratorio de Gobierno) en ciberseguridad.

Acciones:

· Desarrollar

→ Modelos de innovación abierta de investigación aplicada en IAC
→ Modelos de escalamiento
→ Modelos de Internacionalización
→ Concursos para el desarrollo de investigación por encargo en el área de ciberseguridad que requieran de la colaboración Universidad-Industria

· Generar

→ Programa de fortalecimiento de la Industria de la ciberseguridad
→ Programa de emprendimiento en ciberseguridad
→ Material para difusión y capacitación de mejores prácticas para convertir investigación aplicada en ciberseguridad en productos de base científica tecnológicas insertados exitosamente en la Industria.
→ Alianzas importantes entre organismos de seguridad interior y defensa exterior con la industria nacional en el área.

· Presencia activa en ferias y foros de connotación nacional e internacional para dar a conocer y posicionarse en la región a través de los desarrollos alcanzados. Participación en ferias como FIDAE, EXPOMIN, EXPONAVAL, entre otras que permiten posicionar al país como un referente en la región y a nivel global en la generación de diversas capacidades del área de la IAC

Métricas

· Número de:

→ Proyectos activos para fortalecer la ciberseguridad en cierto sector industrial por medio de la IAC multidisciplinaria

→ Instituciones participantes en iniciativas de innovación abierta en ciberseguridad con foco en desarrollo de soluciones, productos o servicios en el área.
→ Proyectos establecidos luego del desafío de innovación abierta
→ Investigaciones realizadas por encargo donde colaboran Universidad e Industria
→ Proyectos de I+D+i de base IAC patrocinados por Estado
→ Productos de IAC en al menos TRL (Technology Readiness Level) nivel 5
→ Productos de IAC con TRL entre niveles 6 y 9
→ Productos de base IAC escalados
→ Negocios alrededor de productos de base IAC
→ Productos de base IAC con salida internacional
→ Licencias (u otro mecanismo de protección de propiedad intelectual) transferidas de forma efectiva para su explotación comercial.
→ Empresas o Startups de base científica-tecnológica nacionales que ofrecen o desarrollan productos o servicios de ciberseguridad para la industria local o internacional
→ Participantes relevantes en eventos

· Porcentaje de investigadores en proyectos de colaboración

· Aumento del Tamaño del sector TIC (Tecnologías de la Información y Comunicaciones) debido a IAC

Programa 3: Laboratorio Nacional Distribuido para la I+D en Ciberseguridad

Pilar: Capacidades de Recursos

Objetivo: Habilitar una infraestructura compartida que permita investigar desarrollar y probar algoritmos/modelos/productos del segmento ciberseguridad para diferentes Industrias optimizando recursos.

Descripción: Aborda la Falta de Infraestructura para desarrollar investigación en ciberseguridad, primero levantando los requerimientos y recursos actuales como base y segundo contrastando lo requerido dada las amenazas futuras prioritarias para el País y tercero facilitando la postulación conjunta a fondos para concursos Fondequip (Fondo de Equipamiento Científico y Tecnológico de ANID).

Acciones previas:

· Identificar mecanismos o estructuras de financiamiento que permitan asegurar la continuidad del desarrollo de capacidades en materias de ciberseguridad y sus diversas áreas de especialización
· Disponibilidad de plataforma para levantar requerimientos de infraestructura existente en términos de recursos de procesamiento
· Identificar geográficamente potenciales nodos que permitan integrar las capacidades de investigación y desarrollo digital nacional.
· Visibilizar la red de infraestructura existente en términos de recursos de Procesamiento y almacenado.

Acciones:

· Crear
→ Laboratorios de Pruebas y Prototipos para proyectos con I+D en Ciberseguridad.
→ Laboratorio nacional distribuido en ciberseguridad.

· Levantar proyectos
→ Emblemáticos sobre Laboratorios que permitan un apalancamiento entre la industria, el Estado y la academia. (equivalente en envergadura al Proyecto Nacional Satelital)
→ Fondequip con asociados

· Generar
→ Programa para que investigadores puedan correr experimentos en IAC a costo 0
→ Una guía de las mejores prácticas para recursos y procesos requeridos para realizar actividad de IAC

· Starter Kit de Infraestructura habilitante para realizar IAC

Métricas

· Número de:

→ Nodos de la red nacional de IAC
→ Nodos que proveen infraestructura

→ Usuarios del Laboratorios de Pruebas y Prototipos
→ Usuarios del Laboratorio Nacional Distribuido
→ Nuevos investigadores financiados indirectamente con los mecanismos
→ Investigadores beneficiados por starter kits
→ Resultados de investigaciones con reconocimiento a estos instrumentos
→ Pruebas de conceptos realizadas en laboratorios
→ Proyectos e iniciativas de desarrollo e investigación por sectores (industria, gubernamental, defensa, retail, banca, etc.) en materias de ciberseguridad que se enfoquen en el desarrollo nacional.

· Porcentajes de
→ Infraestructura mínima necesaria para IAC en diferentes ámbitos
→ Ocupación del Laboratorio Nacional Distribuido
→ Cubrimiento de demandas de requerimiento de infraestructura
→ Satisfacción de starter kit
→ Oportunidades de mejora del starter kit indicados por investigadores y cerrados satisfactoriamente por la comunidad

· Financiamiento e inversiones, para generación de masa crítica de especialistas y dimensión de las capacidades y desarrollo tecnológico alcanzada relativo a la ciberseguridad nacional.
· Fondos adjudicados en Fondequip

Programa 4: Centro Iberoamericano de Investigación de Capacidades de Ciberseguridad (CIICC).

Pilar: Capacidades de Coordinación

Objetivo: Posicionar a Chile como líder en IAC en las 5 dimensiones del CMM de Oxford.

Descripción: Organismo coordinador de la red de centros de investigación, de escalamiento, de difusión que monitorea y ayuda al cumplimiento de la Política nacional de ciberseguridad y se coordina con diferentes organismos del Estado para facilitar el avance de la IAC en Chile a favor de los diferentes estamentos del País, incluido el desarrollo de capacidades humanas. Además, poseer presencia continental, abordando todo el espectro "amplio" de la Ciberseguridad en base a las 5 dimensiones del CMM. Este es el que se relaciona con Oxford

Acciones previas:

· Crear Dashboard Web de

→ La operacionalización de la Política Nacional vigente

→ Actividad de la red de centros de IAC en el País

· Levantar registro nacional de vulnerabilidades conocidas en soluciones/ dispositivos usados en Chile para su adecuado parche (ej. Jira)

· Oficialización de un proceso que facilite la integración de la academia a áreas de desarrollo tecnológico en organismos del Estado.

· Establecer un consorcio de universidades nacionales para crear un centro de capacidades en ciberseguridad, bajo el modelo de la Universidad de Oxford

Acciones:

· Integrar el consorcio de Universidades a la "constelación" de Centros de Capacidades en Ciberseguridad que lidera la Universidad de Oxford, y que componen Australia y Sudáfrica entre otros.

· Crear

→ Ente coordinador de la red de IAC del país para fortalecer las capacidades de ciberseguridad en los organismos y empresas del País.

→ Unidad Pública Gratuita de hacking ético

→ Unidad certificadora de compliance con nivel de ciberseguridad en Software

→ Unidad certificadora de compliance en ciberseguridad para IoT (Internet of Things)

→ Unidad certificadora de compliance en ciberseguridad para dispositivos médicos

→ Unidades operativas para medir el nivel de madurez de países en Ciberseguridad (CMM) habilitados por la Universidad de Oxford para realizar los levantamientos y evaluaciones.

→ Unidad que sea contraparte NIST (National Institute of Standards and Technology USA), para la capacitación gratuita de estándares de ciberseguridad

→ Grupo de Estudio y Definición de Estándares, procedimientos y guías en IAC

· Facilitar con los organismos correspondientes la creación de:

→ Concurso Becas para Doctorados académicos científicos en IAC multidisciplinar (otras disciplinas) y sectores específicos.

→ Concurso ANID Instituto Milenio/centros/Núcleo de Investigación con llamado a la Ciberseguridad,
→ Concursos ANID/Corfo asociado a FONDEF (Fondo de Fomento al Desarrollo Científico y Tecnológico) Idea/Tecnológico temático en ciberseguridad
→ Centro Nacional de Investigación en Ciberseguridad (no adscrito o bajo el alero de una Universidad o Consorcio Universitario) Institución gubernamental similar al INRIA (Instituto Francés de Investigación en Ciencias y Tecnologías Digitales)
→ Programa de importación de expertos internacionales (concurso ANID)
→ Concurso Becas para pasantías de investigadores en centros de IAC internacionales.
→ Prácticas de IAC en áreas de investigación en ciberseguridad
→ Pasantías en Centros Nacionales de Investigación en Ciberseguridad
→ Instancias de pasantías para estudiantes de pre y post grado en la industria nacional e internacional y en entidades gubernamentales, así como en la red de centros para acelerar el desarrollo de capacidades tecnológicas en el país.
→ Desarrollo de incentivos a la colaboración startup-empresa.
→ Convocatoria a Programa de escalamiento y nuevos negocios en torno a resultados de investigación en ciberseguridad (CORFO-ANID)
→ Proyectos cooperación internacional a través de PCI (Programas de Colaboración Internacional) con recursos para Networking, y apoyo de ANID
→ Instrumento de financiamiento para la Atracción de inversión para el crecimiento y desarrollo de la industria de ciberseguridad (ANID)
→ Instrumentos de fomento al patrocinio del Estado a proyectos de I+D+i con financiamiento público o privado, nacional o internacional en materias de Ciberseguridad.
→ Concursos ANID/Corfo asociado a Startup temático en ciberseguridad

· Generar Hackathones para dispositivos IoT /dispositivos médicos o Software desarrollados /usados como parte de una solución en Chile con el fin de detectar vulnerabilidades y generar parches acordemente.

· Apoyar la creación y participar en Norma técnica para el desarrollo o contratación de software en el Estado, acorde a estándares de desarrollo seguro.

Métricas

· Número de:

→ Organismos apoyados
→ Hacking éticos realizados a MiPymes
→ Organizaciones apoyadas por el ente que hayan formado capacidades de defensa
→ Software compliance nivel de ciberseguridad
→ Soluciones que incluyen IoT compliance nivel de ciberseguridad
→ Dispositivos médicos con compliance nivel de ciberseguridad
→ Dispositivos/Soluciones hackeados éticamente
→ Incidentes en registro nacional
→ Startups usando la norma técnica
→ Centros con información fresca en el dashboard Web de centros
→ Becados en IAC
→ Becados en IAC aplicado a sector
→ Núcleos/Institutos en IAC
→ Proyectos FONDEF en IAC
→ Expertos internacionales con estadías superiores a las dos semanas en Chile por iniciativas de las redes de IAC
→ Investigadores seniors beneficiados en pasantías en centros de IAC internacional
→ Investigadores juniores beneficiados en pasantías en centros de IAC nacional
→ Profesionales/estudiantes beneficiados para realizar prácticas
→ Doctores en IAC insertos en Industria % de doctores en IAC insertos en Industria
→ Empresas o Startups de base científica-tecnológica chilenas que ofrecen o desarrollan productos o servicios de ciberseguridad para la industria local o internacional.
→ Proyectos de I+D+i de base IAC patrocinados por el Estado

· Porcentajes de
→ Puntos abordados por la Política documentadas mostrando evidencia de su avance
→ Incidentes resueltos
→ Becados en IAC no técnico.

· Tiempo medio para resolver incidentes

*Capítulo 4_*

Tecnologías emergentes en ciberseguridad para Chile

PARTICIPARON EN LA ELABORACIÓN DE ESTE TEXTO:

- Equipo Coordinador submesa "Tecnologías Emergentes en Ciberseguridad": Rodrigo Alfaro y Luz Cardona

- Comité de Trabajo Técnico de la submesa "Tecnologías Emergentes en Ciberseguridad" convocado por la Comisión formado por: Miguel Solís, Carlos, Bustos, Pablo Itaim, Yerka Yukich, Francisco Correa, Mirko Koscina, Ricardo Dorado, Juan Lopizic, Puppy Rojas, Juan Pablo Gonzalez y Ricardo Soto.

1. INTRODUCCIÓN

La promulgación de la Ley N° 21.180 sobre Transformación Digital del Estado, ha implicado procesos de modernización continuos que han implicado desafíos en diferentes ámbitos, como lo ha sido la de propiciar una cultura hacia el ciudadano digital y a su vez los desafíos en materia de ciberseguridad han requerido y requerirán esfuerzos de coordinación entre lo público y lo privado para la apropiación de tecnologías emergentes, generar alertas preventivas y de incidentes de ciberseguridad.

Debemos identificar aquellas tecnologías que inciden en la ciberseguridad para incorporarlas en la Estrategia de Transformación Digital al 2035. Para ello, debemos conocer el estado del arte en relación con tecnologías emergentes; establecer los desafíos futuros, sus dominios y categorías, para finalmente, a través de un análisis metodológico, proponer incorporar su aplicación y usos.

En más de 12 reuniones de trabajo, desarrolladas entre el 22 de junio y el 30 de noviembre de 2022, un equipo conformado por 13 profesionales de formaciones diversas entre los que se cuentan abogados, ingenieros, periodistas, empresarios, académicos y otros, lograron el resultado que se refleja en este capítulo.

2. CONTEXTO

Entenderemos por **tecnologías emergentes** a aquéllas que tienen el potencial de transformar una industria existente, ya sea por su novedad como por su impacto. Las líneas que se han identificado que vienen trabajando con tecnologías emergentes son las siguientes: Ciberseguridad, Analítica, IoT, Nuevas dimensiones, Inteligencia Artificial, Robótica, Computación en la nube, Blockchain e Impresión 3D (Building the Digital State, 2019 EY Global).

Para el presente trabajo la línea seleccionada sobre tecnologías emergentes es la de ciberseguridad, la cuál será abordada desde el reconocimiento de sus dominios/categorías, para facilitar los campos de su aplicación, su evolución y el futuro de estas.

Los **dominios de ciberseguridad** se refieren a las diversas formas en las que se pueden implementar metodologías de ciberseguridad, las que tienen un alto grado de complejidad y están en constante cambio. La seguridad de las aplicaciones, la seguridad física, la evaluación de riesgos y la inteligencia de amenazas son algunos de los dominios más comunes en la seguridad cibernética.

Cada parte del dominio cibernético tiene su propio conjunto distintivo de desafíos y riesgos de seguridad que deben ser atendidos. Para proteger el dominio cibernético, las organizaciones deben encontrar los desafíos y riesgos asociados con cada subdominio y mitigarlos.

En particular, existe la necesidad de abordar los riesgos de seguridad cibernética desde una perspectiva de sistemas de múltiples escalas, reconociendo las diversas interacciones entre los sistemas cibernéticos, físicos y humanos (Lambert et al. 2013). En esta dirección, es importante enmarcar el problema en términos de resiliencia cibernética, en el que Linkov et al. (2013) discute cómo los tomadores de decisiones requieren la capacidad de planificar las amenazas y absorber, recuperar y adaptarse a estas después de que se produzcan a lo largo de los dominios físicos, de información, cognitivos y sociales en los que existen estos sistemas de múltiples escalas (Zachary A. C., Igor L. y James H. L., 2013).

En el dominio físico se incluyen tanto el hardware como el software y las redes, como componentes básicos de la infraestructura cibernética. Por ejemplo, Gilmore et al. (2013) describió los riesgos que plantean las piezas electrónicas falsificadas en el contexto de la seguridad del hardware.

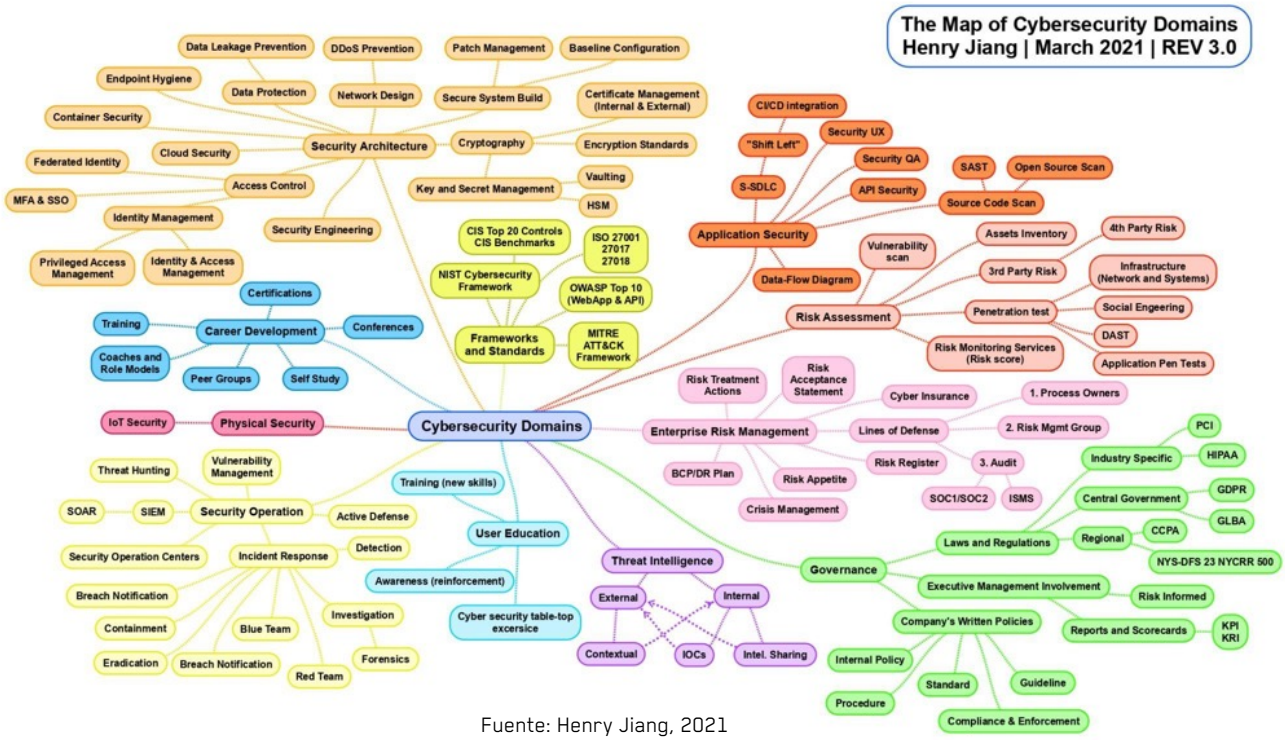
Las características del dominio de la información son: el monitoreo, el almacenamiento de información y la visualización. Primero, Baiardi y Sgandurra (2013) analizaron una metodología de evaluación de riesgos basada en simulación que modela agentes de amenazas adaptativos e identifica contramedidas efectivas. Cam y Mouallem (2013) luego describieron una forma de modelar dinámicamente el aseguramiento de la misión a través del monitoreo de activos cibernéticos e incluyeron un esquema de gestión de riesgos para mitigarlos llevándolos a niveles aceptables. Finalmente, Ezell et al. (2013) describió un marco para modelar los riesgos e impactos de los ataques cibernéticos en los sistemas de control de tráfico.

En el dominio cognitivo, la información debe analizarse y detectarse adecuadamente, así como utilizarse para la toma de decisiones. Por ejemplo, Rosoff et al. (2013) exploró las heurísticas de toma de decisiones mentales que utilizan las personas cuando se enfrentan a un dilema de ciberseguridad. Presentó los resultados de dos experimentos en los que se modificó el marco de ganancia-pérdida para los participantes cuando se les presentaron escenarios de ciberseguridad.

Las decisiones sobre seguridad cibernética deben ser coherentes con las consideraciones sociales, éticas y de otro tipo que son características del dominio social que las envuelve. Algunos autores han trabajado el dominio social, Sheppard et al. (2013) abordaron la seguridad cibernética desde una perspectiva organizacional, describieron cómo las organizaciones pueden estar mejor preparadas para responder a las amenazas cibernéticas y brindaron una encuesta y un cuadro de mando para medir los niveles de preparación. Pawlak y Wendling (2013) luego exploraron las tendencias existentes y futuras en las políticas gubernamentales relacionadas con la ciberseguridad e identificaron brechas y posibles caminos a seguir. Kelic et al. (2013) describió un marco de decisiones basado en agentes para modelar los impactos macroeconómicos de los ataques cibernéticos en sectores industriales vulnerables, como la industria del petróleo y el gas. Vaishnav et al. (2013) describió un marco novedoso que conecta la ciberseguridad y las relaciones internacionales como un sistema único, comentando las propiedades de dicho sistema.

Por otro lado, Jiang, H. (2021) propone un mapa de 11 dominios de la seguridad cibernética con sus respectivos subdominios o categorías (ver Figura 1).

Figura 1: Mapa mental de dominios y subdominios en ciberseguridad.



Fuente: Henry Jiang, 2021

Para los dominios trabajados se adoptó la siguiente descripción:

1. Arquitectura de seguridad (Security Architecture): El dominio de la Arquitectura de seguridad hace referencia a un plan y un conjunto de principios que describen los servicios de seguridad que un sistema debe proporcionar para satisfacer las necesidades de sus usuarios, los elementos del sistema para implementar los servicios y también los niveles de rendimiento que se requiren en los elementos. para hacer frente al entorno de amenazas. El dominio a su vez considera otros 23 subdominios.

2. Operaciones de seguridad (Security Operation): El dominio de Operaciones de seguridad se enfoca principalmente en detectar y proteger información confidencial y crítica para el negocio dentro de cualquier organización. Algunas de sus funciones incluyen: búsqueda de amenazas, respuesta a incidentes, información sobre amenazas y análisis forense.
El dominio a su vez considera otros 16 subdominios

3. Gobernanza (Governance): La Gobernanza de la seguridad de TI es el sistema mediante el cual una organización dirige y controla la seguridad de TI (adaptado de ISO 38500). La gobernanza de la seguridad de TI no debe confundirse con la gestión de la seguridad de TI. La gestión de la seguridad de TI se preocupa por tomar decisiones para mitigar los riesgos; la gobernanza determina quién está autorizado a tomar decisiones. La gobernanza especifica el marco de rendición de cuentas y proporciona supervisión para garantizar que los riesgos se mitiguen adecuadamente, mientras que la gestión garantiza que se implementen controles para mitigar los riesgos. La gobernanza garantiza que las estrategias de seguridad estén alineadas con los objetivos comerciales/estratégicos y sean consistentes con las regulaciones. El dominio a su vez considera otros 20 subdominios

4. Gestión de Riesgos empresariales (Enterprise Risk Management): Un programa ERM puede ayudar a aumentar la conciencia de los riesgos comerciales en toda la organización, infundir confianza en los objetivos estratégicos, mejorar el cumplimiento de los mandatos de cumplimiento normativo e interno y mejorar la eficiencia operativa a través de aplicaciones más consistentes de procesos y controles. El dominio a su vez considera otros 13 subdominios.

5. Seguridad Física (Physical Security): La Seguridad física describe las medidas diseñadas para garantizar la protección física de los activos de TI, como instalaciones, equipos, personal, recursos y otras propiedades, contra daños y accesos físicos no autorizados. Se toman medidas de seguridad física para proteger estos activos de amenazas como: robos, vandalismo, incendios y desastres naturales. El dominio a su vez considera un subdominio.

6. Desarrollo de la Carrera (Career Development): Los profesionales de la ciberseguridad trabajan en empresas e industrias de todos los tamaños para proteger a las organizaciones de ataques y filtraciones de datos.
El dominio a su vez considera otros 6 subdominios.

7. Inteligencia de Amenazas (Threat Intelligence): La inteligencia de amenazas, también conocida como inteligencia de amenazas cibernéticas (CTI), es información organizada, analizada y refinada sobre ataques potenciales o actuales que amenazan a una organización. El propósito principal de la inteligencia de amenazas es ayudar a las organizaciones a comprender los riesgos de las amenazas externas más comunes y graves, como las amenazas de día cero, las amenazas persistentes avanzadas (APT) y los exploits. El dominio a su vez considera otros 5 subdominios.

8. Evaluación de Riesgos (Risk Assessment): La Evaluación de los riesgos de seguridad cibernética identifica los diversos activos de información que podrían verse afectados por un ataque cibernético (como hardware, sistemas, computadoras portátiles, datos de clientes y propiedad intelectual), y luego identifica los diversos riesgos que podrían afectar esos activos. El dominio a su vez considera otros 10 subdominios.

9. Marcos y Estándares (Framework & Standard): El Marco es una guía voluntaria, basada en estándares, pautas y prácticas existentes para que las organizaciones administren mejor y reduzcan el riesgo de seguridad cibernética. Además de ayudar a las organizaciones a gestionar y reducir los riesgos, se diseñó para fomentar las comunicaciones de gestión de riesgos y ciberseguridad entre las partes interesadas internas y externas de la organización. El dominio a su vez considera otros 5 subdominios

10. Seguridad de las aplicaciones (Application Security): La Seguridad de las aplicaciones es el proceso de desarrollar, agregar y probar funciones de seguridad dentro de las aplicaciones para evitar vulnerabilidades de seguridad contra amenazas, como el acceso y la modificación no autorizados. El dominio a su vez considera otros 10 subdominios

11. Educación del usuario (User Education): La Educación del usuario propende por una entrega sistemática de programas de concientización y capacitación que brinden experiencia en seguridad y ayuden a establecer una cultura consciente de la seguridad. El dominio a su vez considera otros 3 subdominios

A partir de los 11 dominios anteriores se realiza un trabajo de revisión de su aplicación e identificación de empresas que pudieran estar trabajando en dichos campos en el ámbito nacional, y para algunos casos la revisión del nivel de madurez de la tecnología emergente seleccionada.

Por otro lado, en el reporte de "Cyber Defenders 2021", se presentaron 14 categorías que guiarán el futuro próximo de las empresas dedicadas o que se dedicarán a la ciberseguridad: "Identity orchestration, Data Firewalls, Security creds, Outsourced security, SaaS security, Crypto defense, Security-infused networks, Cyber automation, API Protection, Cyber Insurance, Shift Left Security, Secure Data Sharing, Auto Security, Post Quantum cryptography". A continuación, se presentan algunas reflexiones al respecto que se están dando en la actualidad:

1. Identify orchestration (orquestación de Identidad): Las organizaciones que operan en sistemas locales y múltiples nubes carecen de una solución única y unificada para administrar la identidad y limitar el acceso a datos y sistemas.

2. Data Firewalls (Firewalls de Datos): Las organizaciones enfrentan costos financieros y de reputación cuando los piratas informáticos roban sus datos o se filtran al público.

3. Security creds (Credenciales de Seguridad): Las infracciones pasadas han puesto de relieve que una organización es tan fuerte como su socio más débil. Al adaptarse a este nuevo panorama de amenazas, las organizaciones buscan diferenciarse de la competencia y ganar negocios al exhibir sus credenciales de seguridad.

4. Outsourced security (Seguridad subcontratada): Administrar múltiples proveedores, mantenerse actualizado sobre las últimas tecnologías y amenazas, y contratar talento calificado puede sobrecargar a los equipos de seguridad corporativos.

5. SaaS security (Seguridad SaaS): Las organizaciones de todas las industrias han aumentado el uso de aplicaciones SaaS, o software de terceros que se ejecutan en la nube, en los últimos años, lo cual implica riesgos adicionales en ciberseguridad.

6. Cryptodefense (Cripto Defensa): Si bien blockchain tiene propiedades que respaldan la seguridad y la privacidad no es inmune a los ataques de ciberseguridad.

7. Security-infused networks (Redes embebidas con seguridad): Las empresas dependen de redes confiables para habilitar una fuerza de trabajo remota efectiva. Históricamente, estas redes se han protegido con numerosas soluciones puntuales (P.ej: , VPN, firewalls, agentes de seguridad de acceso a la nube), que pueden frustrar a los equipos y empleados de TI.

8. Cyber Automation (Automatización cibernética): Los ciberataques, las alertas y las vulnerabilidades siguen aumentando, mientras que la oferta de profesionales cualificados en ciberseguridad sigue siendo limitada. Este desequilibrio desafía a las empresas que buscan proteger sus sistemas y datos.

9. API Protection (Protección API): El uso de la interfaz de programación de aplicaciones (API) se ha disparado en todas las industrias en los últimos años. Esto trae riesgos de seguridad que requieren nuevas protecciones.

10. Cyber Insurance (Seguro cibernético): Las violaciones de datos de todos los tamaños se han vuelto más costosas en los últimos 3 años.

11. Shift Left Security (Seguridad Shift Left): Cuando se trata de desarrollo de software, las consideraciones de seguridad suelen ser el último paso antes del lanzamiento. La creación de software sin tener en cuenta la seguridad puede, en el mejor de los casos, provocar retrasos e ineficiencias y, en el peor de los casos, crear vulnerabilidades graves.

12. Secure Data Sharing (Uso compartido de datos seguros): Para hacer uso de los datos (p. ej., identificar nuevos tratamientos en medicina, desarrollar perfiles de clientes en el comercio minorista, etc.), las empresas pueden buscar compartir, combinar y analizar información confidencial. Proteger estos datos compartidos mientras se cumplen los estándares regulatorios presenta un desafío.

13. Auto Security (Seguridad Automática): A medida que los vehículos adoptan nuevas tecnologías y se convierten efectivamente en centros de datos sobre ruedas, crean nuevas oportunidades para los piratas informáticos.

14. Post Quantum cryptography (Criptografía post cuántica): A medida que se desarrolle la computación cuántica, eventualmente podrá descifrar los métodos actuales de encriptación de clave pública.

Según estudios de Gartner (2021), las tecnologías emergentes en ciberseguridad vienen generando impactos importantes en las organizaciones (ver Tabla 1).

Tabla 1. Tendencias de tecnologías emergentes.

	Hoy	1 a 3 años	3 a 6 años	6 a 8 años
Business Enablers	• Low-code Application Platform (LCAP)	• Application Ecosystmes	• Smart Contract • Productuzation of Data • Distributed Ledgers • Packaged Business Capabilities • Distributed Cloud • Tokenization • mmWave 5G	• AR Cloud • AI-Generated Composite Applications
Productivity Revolution	• Deep Neural Networks • Cloud AI Developers Services • Edge AI	•	• Model Compression • Composite AI	•
Interfaces and Experiences	• Advanced Computer Vision	• Transformers-Based Language Models • Advanced Virtual Assistants	• Smart Personalization • IoT Platforms • Digital Twin	•

Fuente: Basada en Gartner, 2021

3. DESAFÍOS FUTUROS

3.1. Quantum Computing (QC)

La Computación Cuántica (o Quantum Computing) es un área de la informática surgida a principios de los años 80's que se basa en los principios de la teoría cuántica, que comprende el comportamiento de la materia, energía e información a nivel subatómico, para desarrollar nuevos sistemas que permiten operar más rápido y más eficientemente.

El impacto de la Computación Cuántica en la ciberseguridad puede focalizarse en la criptografía, donde ya se plantea la necesidad de trabajar con criptografía post-cuántica.

3.2. Artificial Intelligence (AI)

La Inteligencia Artificial es un área de la informática, surgida a mediados de los años 50's, que estudia sistemas capaces de percibir su entorno y realizar acciones que maximizan sus posibilidades de lograr sus objetivos. Dentro de esta área existe una sub área denominada Aprendizaje de Máquinas (o Machine Learning), que plantea que las máquinas pueden reconocer patrones a partir del análisis de datos históricos, los que usan como ejemplos para parametrizar sus modelos y que una vez aplicados, sus resultados sean similares a los que en realidad ocurrieron. A partir de esto, es posible automatizar decisiones según el ajuste al patrón definido.

El impacto de la Inteligencia Artificial en la ciberseguridad puede focalizarse en el reconocimiento de patrones, a través del cual, es posible clasificar objetos, detectar anomalías y predecir comportamientos de usuarios.

3.3. Web 3.0 (Blockchain y Metaverse)

Se denomina Web 3.0 a la red informática donde se conectan máquinas y humanos para procesar datos y generar contenido de modo simple y rápido. Se basa en el análisis de datos y máquinas accesibles e inteligentes, mediante servicios descentralizados utilizando tecnología de blockchain y redes P2P[1] (Peer to Peer)

El impacto de la Web 3.0 en la ciberseguridad radica en su facilidad para asegurar mayor privacidad y seguridad, procurando mantener una experiencia personalizada. De forma más específica aún y dado el impacto que puede tener de manera directa en el bienestar de cada usuario, las aplicaciones basadas en Blockchain antes de salir a producción, deberían cumplir criterios mínimos de seguridad a la vez que se establecen políticas regulatorias y procedimientos en caso de identificar vulnerabilidades, en beneficio del resguardo del usuario final.

[1] https://es.wikipedia.org/wiki/Peer-to-peer

3.4. Cyberphysics Systems: Industrial Internet of Things (IIoT), IoT (Internet de las Cosas)

Los sistemas ciber físicos integran capacidad de procesamiento, almacenamiento y comunicación con el objetivo de monitorear y posiblemente controlar variables físicas del entorno. Este tipo de sistemas forman la base del IoT[2] (Internet of Things), y el IIoT[3] (Industrial Internet of Things), donde dispositivos electrónicos se comunican con objetos, personas u otros dispositivos conectados a Internet. Al involucrar la comunicación automática de datos relativos a personas, como se hace a través de dispositivos vestibles, se llega a lo que se conoce como IoE[4] (Internet of Everything).

El impacto en la ciberseguridad de los sistemas ciber físicos, y en especial IoT y sus derivados, puede focalizarse en la seguridad de la comunicación e integridad de los datos transmitidos a través de la red de dispositivos, ya que estos datos pueden tener relación con información sensible y el eventual secuestro de dispositivos podrían afectar de manera directa y crítica al proceso intervenido, lo que en un ambiente industrial cobra especial relevancia.

3.5. Industry 4.0 y Cloud platforms (CP)

Se denomina Industria 4.0 a la introducción de las nuevas tecnologías digitales en los procesos de producción industrial. Implica el uso de sistemas informáticos y diversos tipos de sensores con el objetivo de mejorar la eficiencia del negocio y poder ejercer un mayor control de este. Estas tecnologías se basan en la integración de procesos más modernos en las plantas de producción, y entre estas se encuentran: Big Data, Cloud Computing, Robótica, Internet de las Cosas y Realidad Aumentada.

En este escenario de irrupción de las tecnologías digitales en los procesos de producción de las organizaciones, alcanza mayor relevancia la ciberseguridad.

3.6. Neurotechnology

Se denomina Neurotecnología a las tecnologías enfocadas en comprender el trabajo del sistema nervioso humano, especialmente el cerebro, y que permiten desde la visualización sus procesos internos hasta la alteración, control, reparación o mejoramiento de sus funciones. Para ello utiliza otras tecnologías como la Inteligencia Artificial y los Sensores.

Si bien, existen tecnologías en este ámbito hace décadas, el creciente desarrollo e interés de estas tecnologías ha generado polémicas en cuanto a la posibilidad de alterar sistemas para controlar humanos.

[2] https://es.wikipedia.org/wiki/Internet_de_las_cosas
[3] https://en.wikipedia.org/wiki/Industrial_internet_of_things
[4] https://www.computerweekly.com/es/definicion/Internet-de-todo-IoE

3.7. Capital Humano para identificar riesgos e implementar cambios. Regulación oportuna. Formación.

El Capital Humano es clave para plantearse una revolución cultural en la cual el centro son las personas. Se debe comenzar por el perfeccionamiento y la profesionalización del equipo humano de modo de mejorar el abordaje y mantenerse actualizado. Lo anterior debe ir de la mano con la identificación de nuevas habilidades profesionales requeridas y el rediseño de los modelos de trabajo.

4. PROPUESTA

4.1. Metodología para estructurar lineamientos de ciberseguridad y gestionar las innovaciones

Cómo enfrentar nuevos desafíos (framework) Considerando que la aplicación de tecnologías emergentes en cierto negocio o industria usualmente involucra inversiones que pueden impactar de manera profunda, y, por otro lado, dado que no todas las tecnologías emergentes trascienden en el tiempo, es necesario primero analizar su impacto, relevancia y potencial.

Para analizar el potencial de cierta tecnología emergente, se sugiere hacer una nueva identificación del problema que dicha tecnología pretende abordar, ya que con frecuencia una innovación cambia la perspectiva desde la que se mira el problema. Además, a pesar de que sea posible proyectar el avance de la tecnología en el tiempo, con el objetivo de mantener su potencial de aplicación en un entorno realista, se debe mantener en vista la factibilidad técnica de poder llevar a cabo soluciones basadas en dicha tecnología emergente, considerando los recursos y avance tecnológico actual.

Un framework se puede entender como un diseño reutilizable, ya sean modelos y/o código, que puede ser especializado y ampliado para proporcionar una parte de la funcionalidad general de muchas aplicaciones (ISO/IEC/IEEE, 2010). Para este trabajo se define framework como un diseño reutilizable compuesto de un análisis metodológico.

4.2. Metodología para gestionar innovaciones

Con base en la literatura revisada y el contexto descrito anteriormente, se plantea la siguiente propuesta metodológica de framework para gestionar innovaciones a partir de tecnologías emergentes en la línea de la ciberseguridad.

Los objetivos de la Metodología son los siguientes:

1) Generar un proceso estándar que permita adoptar tecnologías emergentes

2) Identificar y validar tecnologías emergentes

3) Apropiación de la tecnología emergente

4) Generar capacidades en el país para afrontar las amenazas y ataques en materia de ciberseguridad

El enfoque metodológico que se propone puede partir a través de responder las siguientes preguntas:

* **¿Por qué?** Esta pregunta estaría asociada a las necesidades de la organización que motivan el uso de las nuevas tecnologías.

* **¿Qué** debe considerarse para implementar las tecnologías emergentes, una vez se tiene claro su propósito de uso?

* **¿Cómo** adoptar y hacer uso de las tecnologías emergentes mediante el apalancamiento en las capacidades, arquitectura y estructura de las organizaciones que buscan implementar estas tecnologías?

Como etapas para la implementación, se proponen las siguientes:

1. Generar Estrategias: Desarrollar estrategias que conduzcan a la implementación de la tecnología emergente.

Las tecnologías emergentes cumplirán su misión cuando el driver de implementación esté alineado a un objetivo, problema o necesidad de la organización.

a. Análisis de la tecnología emergente a implementar. Analizar cuáles objetivos podrían estar soportados en las tecnologías emergentes, qué problemas no han sido resueltos con tecnologías clásicas/tradicionales.

b. Análisis del entorno interno/externo de la organización y la reglamentación/regulación vigente.

c. Proceso de Categorización: Identificación del dominio/categorías con el cual estará relacionada.

d. Revisión de su nivel de madurez a través de la metodología de TRLs (Technology Readiness Levels).

e. Identificación de los casos de uso: La identificación de casos de uso facilitará el entendimiento sobre las nuevas tecnologías, en el sentido que estas serán compendiadas desde su aplicabilidad y no desde un lenguaje técnico. El identificar y priorizar los casos de uso correctos ayudará a ofrecer el máximo valor en su implementación.

f. Identificación de las empresas que pueden proveer la tecnología emergente: Se sugiere que debe propiciarse que en el país se genere capacidad instalada.

g. Verificación de viabilidad: Verificar los beneficios que se quieren alcanzar versus los esfuerzos necesarios para implementar la tecnología emergente. Por otro lado, la verificación de la viabilidad está en relación con el nivel de madurez de la tecnología emergente, con los casos de uso que debe cubrir y con los riesgos asociados.

2. Diseñar:

a.Establecer los requisitos previos para implementar la tecnología emergente: Determinar los habilitadores para realizar pruebas piloto y determinación de capacidades necesarias para realizar dichas pruebas, recurso humano capacitado, identificación de aliados, ambientes necesarios para llevar a cabo las pruebas, entre otros.

b. Analizar el estado actual de la Organización en relación con esta tecnología y sus requisitos.

c. Programar y desarrollar un piloto

3. Instalar:

a. Establecer la arquitectura, habilitando las capacidades necesarias para su implementación, como lo son: proceso de innovación, experiencias con usuarios, riesgos, talento humano requerido, entre otros aspectos.

b. Gobernanza: Establecer un modelo de gobernanza efectivo el cual permitirá mantener y/o actualizar las innovaciones generadas a través del uso de las tecnologías emergentes.

4. Implementar:

a. Poner a prueba el marco de gobierno establecido y las soluciones diseñadas.

b. Seguimiento, mantenimiento y control: Medir los resultados de la implementación de la tecnología emergente, retroalimentar el proceso y realizar cambios/ajustes cuando sea requerido.

Resumen Funciones:

Etapas	Estrategias	Operacionalización
Generar Estrategias	-Análisis de la tecnología emergente -Verificación de viabilidad	-Categorización -Nivel de Madurez -Identificación casos de uso
Diseñar	-Requisitos previos -Análisis entorno	-Piloto
Instalar	-Arquitectura -Gobernanza	
Implementar		-Comprobar -Seguimiento, mantenimiento y control

5. CONCLUSIONES

El alto nivel de digitalización que existe hoy día, junto con la continua profusión de nuevas tecnologías, genera importantes vulnerabilidades de los sistemas, que son explotadas por ciberdelincuentes para la realización de ataques con el fin de interrumpir el servicio, el robo o secuestro de la información almacenada o la suplantación de identidad, entre otras. Estos ataques suponen graves pérdidas en todos los sectores, vulneración de información confidencial y/o afectaciones importantes en la seguridad de un país.

La ciberdelincuencia crece en la medida que rápidamente los ciberdelincuentes tienen la capacidad de adopción de nuevas tecnologías, el constante crecimiento de usuarios en línea, la mayor facilidad para cometer delitos informáticos y la sofisticación financiera de los ciberdelincuentes al monetizar los delitos cometidos.

La ciberseguridad, como disciplina interdisciplinar naciente, requiere una contextualización y empuje para abrirse a diferentes perspectivas y saberes vinculados a otras disciplinas como lo son las ciencias políticas, la economía, el derecho, las ciencias biológicas y médicas para que se pueda caracterizar un bien común, con visión transversal y con implicaciones globales (Ramírez, 2017).

Lo anterior demandará el desarrollo de una postura interdisciplinar, que reconozca lo límites propios de las disciplinas, experiencias y saberes previos, para abordar una realidad emergente, compleja y con incertidumbres, y así, explorar las nuevas circunstancias que plantea el nuevo escenario digital, construyendo propuestas que puedan responder a los nuevos desafíos.

En este sentido, las tendencias del mundo ilustran cómo la conectividad habilitará posibilidades y presentará también nuevas amenazas que estarán más allá de los estándares tradicionales y buenas prácticas de seguridad y de control.

En consecuencia, el desarrollo de una cultura de ciberseguridad y su regulación deberán ser prioritarias para contener y actuar sobre delitos cibernéticos y, por otro lado, adoptar tecnologías emergentes que propendan por la seguridad nacional y de defensa de los diferentes sectores.

*Capítulo 5_*

Operadores de Servicios Esenciales

PARTICIPARON EN LA ELABORACIÓN DE ESTE CAPÍTULO:

- Equipo Coordinador submesa "Operadores de Servicios Esenciales": Eduardo Morales e Igor Carrasco

- Comité de Trabajo Técnico de la submesa "Operadores de Servicios Esenciales" convocado por la Comisión formado por Patricio Leyton, Igal Neiman, Fernando Muñoz, Juan Huechucura, Marcelo Wong, Mauricio Cartergiani, Carlos Fuentes, Jorge Rojas, Pamela Calisto, Cristian Rojas, Paz Suarez, Freddy Macho

1. INTRODUCCIÓN

Entendemos que un servicio esencial es aquel cuya afectación o interrupción tiene un impacto perturbador en el normal funcionamiento de la defensa nacional, la sociedad o la economía, y que son parte integrante de lo que denominamos Infraestructura crítica.

La prestación del servicio depende de las redes y sistemas de información, y un incidente de ciberseguridad tendría un impacto perturbador en la prestación del mismo.

El impacto de una disrupción debe considerar los siguientes factores: Los usuarios potencialmente afectados, la interdependencia con otros servicios con igual calificación, la afectación de la vida, integridad o salud de las personas, afectación de la actividad económica, extensión geográfica del mismo, y la importancia del servicio.

El concepto de Infraestructuras Críticas (IICC) reviste no solo el aspecto físico o material, sino los aspectos como los equipos de comunicaciones y los sistemas de información, es decir, lo que usualmente denominamos, lo virtual. Una infraestructura crítica puede contener o no Servicios Esenciales (SSEE), dependiendo de su función o propósito. Asi por ejemplo, un puente caminero puede tener el carácter de solo IICC, y un aeropuerto tiene una gran infraestructura física pero para que sea operacional requiere de un conjunto complementario de operadores esenciales que permiten su funcionamiento.

En más de 15 reuniones de trabajo, tanto plenarias como temáticas desarrolladas entre el 15 de agosto y el 20 de noviembre de 2022, un equipo conformado por profesionales de formaciones diversas entre los que se cuentan abogados, ingenieros, periodistas, empresarios, académicos, policías y militares, lograron el resultado que se refleja en este capítulo. En él se reúnen conceptos y ejemplos obtenidos de las políticas implementadas por otros países. El propósito final es estructurar una política fomentando la colaboración entre el sector público-privado.

2. CONTEXTO EN CHILE

La masificación en el uso de Internet, las Tecnologías de Información y Comunicaciones (TIC) y el Internet de las Cosas se han ido masificando en las organizaciones tanto públicas como privadas a nivel mundial, e incluso su implementación ha llegado a las infraestructuras que sostienen los servicios esenciales de los países para mejorar su productividad y eficiencia, siguiendo la tendencia de la Industria 4.0 y la Transformación Digital que está llegando a todos los sectores de la economía y la sociedad.

De esta forma las infraestructuras críticas de hoy en día se vuelven mucho más vulnerables que antes dado que aumenta la superficie de ataques producto de los dispositivos y sistemas digitalizados que son parte de las IICC (Infraestructuras Críticas) y que poseen vulnerabilidades y amenazas potenciales impredecibles. A esto se debe agregar la Protección y Gobernanza de los datos críticos operacionales y datos personales, que muchos IICC poseen y en las que actualmente existe una baja madurez de la gestión de sus datos.

A nivel mundial, si analizamos el alto número de ataques tanto a la infraestructura física como a la virtual asociada al ciberespacio, se observan al menos tres principales motivos o causa raíz que son: Dinero, Poder y Subversión.[5] Importante destacar que los grupos asociados a cada causa raíz son distintos: Dinero (Cibercrimen Organizado), Poder (Ciberejércitos de países que no se encu entran alineados a nuestra visión como país) y Subversión (Ciberterroristas o Grupos Hacktivistas). El poder distinguirlos, permite saber lo que persigue cada uno de estos grupos, para así tomar las estrategias y medidas necesarias para cada caso.

De acuerdo al último reporte elaborado por la CEPAL[6], se indica que la industria del cibercrimen ha aumentado en complejidad, a través del uso de herramientas de Machine Learning y de Inteligencia Artificial (IA), y en volumen, a través del mercado de malware como servicio (MaaS) ofrecido en la Deep Web. Al mismo tiempo, la pandemia ha llevado a un incremento anual del tráfico total en internet, y ha cambiado sus hábitos de uso. Al mismo tiempo, en la región dan por resultado un aumento interanual para el mes de octubre de 2020 de 67% de ataques de ransomware, 71% de malware a través de páginas web seguras y de 510% para ataques a dispositivos de internet de las cosas (según Sonicwall, 2020).

Este escenario emergente encontró a los distintos países de la región con diferentes grados de maduración en ciberdefensa, registrándose este efecto tanto en el ámbito privado como público. Como una muestra de ello

[5] Plan Director de Ciberseguridad para el Sector Eléctrico 2021-2023, Cigré Chile Septiembre 2020.
[6] Estado de la ciberseguridad en la logística de América Latina y el Caribe, serie Desarrollo Productivo, N° 228 (LC/TS.2021/108).

los países más afectados por incidentes de seguridad en empresas de logística son Brasil y Chile. Logística que por cierto está presente en todos los sectores estratégicos con infraestructuras críticas, y operadores de servicios esenciales.

Ahora, desde un punto de vista de la Protección de los Servicios Esenciales de la población, claramente la Ciberseguridad cumple un rol fundamental, dado que detrás de estos servicios esenciales existen infraestructuras de carácter crítico para el desarrollo económico y social de los países y, además, estas infraestructuras actualmente poseen sistemas ciber-físicos que se conectan al ciberespacio para su mayor eficiencia y productividad, pero que nos deja en una posición vulnerable, que obliga a ampliar los ámbitos de acción en materia de protección.

3. ANÁLISIS DE ENTORNO Y ESTÁNDARES EN IICCY SSEE EN CHILE

La implantación de estándares y estrategias de ciberseguridad a nivel global en las denominadas IICC y/o SSEE, como son la industria bancaria, de telecomunicaciones, o el sector de generación, transmisión y distribución de energía eléctrica en Chile, ayudan en la prevención y respuesta de posibles situaciones de amenazas, vulnerabilidades o ciberincidentes, capacitando a las compañías implicadas en una cultura de resiliencia cibernética y respuesta más eficiente, y con el menor impacto posible sobre usuarios y organizaciones que dependen de ellas.

El ejemplo de esta última permite visualizar algunos aspectos de relevancia: la gestión y producción de energía eléctrica ha evolucionado a lo largo de los años con el fin de satisfacer una demanda, cada vez más creciente con altos niveles de disponibilidad, lo que ha implicado una transformación digital de los modelos en desarrollo con la incorporación de nuevas tecnologías y mecanismos de control.

Si bien lo anterior ha ido permitiendo cumplir con estas necesidades, se ha introducido por la propia naturaleza de las tecnologías implicadas, nuevas debilidades y vulnerabilidades que deben ser gestionadas de forma correcta con el fin de mitigar riesgos, y donde la inmersión en el ciberespacio es el denominador común.

Estos complejos sistemas, por otra parte son generalmente blanco de sofisticados ataques por parte de grupos y organizaciones criminales.

El estándar NERC-CIP, por sus siglas North American Electric Reliability Corporation y CIP que significa Critical Infrastructure Protection, y cuyo principal objetivo es el establecer un conjunto de requisitos específicos para la gestión de seguridad de las IICC y SSEE vinculadas a la producción y gestión de las redes eléctricas. Es el estándar en ciberseguridad que aplican las empresas del rubro en EE. UU., Canadá y parte de México, así como en varios países de Latinoamérica como: Colombia, Ecuador, Brasil, Chile y Perú, y que está siendo implementado por organizaciones responsables de la producción, gestión y/o coordinación de la operación de las redes eléctricas.

La adopción, implementación y despliegue de un estándar en sí mismo no resuelve la compleja dinámica en la cual se desenvuelven los actores que están detrás de las amenazas y de los ciberataques. Ha quedado demostrado que estos grupos globalizados y organizados pretenden generar daño en la cadena de valor de la industria eléctrica y desestabilizar la infraestructura energética de uno o más países.

Buenas prácticas y estándares de protección ayudan a generar las bases sobre las cuales instalar estrategias y controles operacionales que en su conjunto y de manera sistémica permiten ir mejorando progresivamente la resiliencia energética a nivel país y continental.

El sector eléctrico nacional, lleva algun tiempo mejorando los índices de madurez de la ciberseguridad industrial en las entidades coordinadas, tomando estándares internacionales como el NERC CIP y Protocolos de Notificación de Incidentes de Ciberseguridad y el Monitoreo Continuo de un Plan Estratégico de Ciberseguridad e Infraestructura Crítica para el Sector Eléctrico de corto, mediano y largo plazo.

Al hacerlo de esta forma, han establecido un ejemplo para la mejora continua de los inveles de seguridad, en especial la ciberseguridad industrial, transformándose en el referente obligado para el resto de los sectores industriales, IICC y SSEE vinculados.

4. BRECHAS Y RECOMENDACIONES DE SEGURIDAD EN IICC Y SSEE.

Se hace evidente que el desarrollo de la ciberseguridad presenta notables avances en las denominadas redes administrativas y sistemas operacionales antes que en las redes industriales, Scada (Supervisory Control And Data Acquisition: es un concepto que se emplea para realizar un software para ordenadores que permite controlar y supervisar procesos industriales a distancia) y OT (Operational Technology : tecnología operativa que comprende tanto hardware y software que detecta o provoca un cambio, a través de la supervisión y/o el control directo de los equipos, activos, procesos y eventos industriales). Esto ha sido una tendencia mundial, donde

tanto ciberataques recurrentes como las exigencias históricas de cumplimiento de estándares de ciberseguridad a sectores con alta exposición de datos personales y alto volumen de transacciones de datos como el sector financiero, retail, e-commerce, ha impulsado el desarrollo de una amplia gama de soluciones.

En cambio, en el sector industrial e IICC, ha habido un rezago en la materia. Prueba de ello es como las grandes instituciones financieras o comerciales tienen en forma mandatoria personal como un CISO (Oficial de Seguridad de la Información), mas esta situación no necesariamente se da en el contexto referido.

La internalización de la ciberseguridad en la alta dirección del sector industrial y de servicios, tanto en las medianas como en las grandes empresas está dando pie a la creación de áreas especializadas e incorporación de personal especialista, incluido un oficial de ciberseguridad, cuyas funciones iniciales son las redes administrativas, para luego incorporar, en forma incipiente, los riesgos propios de la ciberseguridad industrial que implican vulnerabilidades en maquinarias en línea, sistemas Scada, IoT (Internet of Things: objetos físicos con sensores, capacidad de procesamiento, software y otras tecnologías que se conectan e intercambian datos con otros dispositivos y sistemas a través de internet u otras redes de comunicación) y robots entre otros.

Con una interconexión creciente, se dificulta concebir operaciones que sean aisladas, puesto que una gran cantidad de equipos y sistemas tienen capacidades de comunicación y proceso para facilitar el funcionamiento continuo. Sin embargo, esta interconexión también representa un vector de posibles ataques cibernéticos que pueden afectar operaciones por períodos de tiempo indeterminados que pueden ir desde algunas horas a días o incluso a semanas, tal como ocurrió en otros países en Norsk Hydro[8] o Mondelez[9], causando daños en ambos casos por sobre los US$100 millones. Los equipos industriales pueden incluso venir "infectados" desde la misma fábrica de origen (bajo la lógica del "caballo de troya") y una vez instalado en la planta industrial y/o de infraestructura crítica se puede propagar hacia el resto de la operación, como ocurrió con las centrifugas de Uranio en Irán.

Existen organizaciones de IICC y SSEE han establecido políticas operacionales tendientes a separar sus redes industriales de las redes administrativas, a fin de evitar o mitigar la propagación de posibles ciberataques y sus efectos operacionales. Desafortunadamente las soluciones de ciberseguridad para las redes OT son poco conocidas y desarrolladas lo que ha generado brechas en su incorporación efectiva.

[7] https://ics-cert.kaspersky.com/publications/news/2019/03/22/metallurgical-giant-norsk-hydro-attacked-by-encrypting-malware/

[8] https://www.leonoticias.com/comarcas/ciberataque-nivel-internacional-20170627190313-nthtml?ref=https%3A%2F%2Fwww.google.es

Por otra parte, el nivel de cibercultura y conciencia de ciberseguridad, así como el conocimiento sobre los potenciales impactos que implica ser víctima de ciberataques, en nuestro país es bajo sin más ambajes. Prueba de lo anterior es que figuramos entre los países con más ataques de phishing per cápita en el mundo[9], reportándose que más de 2 de cada 10 chilenos ha sido víctima de phishing en un período de un año.

La experiencia internacional, reflejada en múltiples publicaciones sobre ciberseguridad ,coincide en señalar que las empresas e instituciones han buscado la manera de mejorar sus estándares y niveles de madurez en ciberseguridad, solo después de uno de estos 3 eventos:

i) La misma institución ha sufrido un ciberataque;
ii) Una institución similar o personas conocidas han sufrido un ciberataque;
iii) El regulador lo ha exigido.

Sobre todo en este último caso, la reacción ha sido la de impulsar programas internos de ciberseguridad para "al menos" cumplir con las exigencias regulatorias. Aun muchos ven la ciberseguridad como un gasto, y no una inversión que permite nos sólo cuidar sus activos, sino defenderse de un potencial daño reputacional.

Otros países con niveles de ciberseguridad más elevados como lo son Israel y España, por citar algunos, han abordado el tema con un enfoque dual, tanto de cumplimiento de estándares, como de matriz de riesgos. Se identifican aquellas situaciones específicas que pueden afectar la ciberseguridad de una IICC o SSEE, así como las medidas mitigadoras, tanto de personas, procesos y tecnologías. Lo anterior, permite acotar tanto la probabilidad de ocurrencia como los efectos indeseados de un potencial ataque. Esto tiene la ventaja de focalizar el uso de recursos, considerando que es imposible obtener la invulnerabilidad total de los sistemas.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) del Departamento de Seguridad Nacional de USA, publicó un conjunto de mejores prácticas de seguridad cibernética para ICS, que la agencia reconoce que son importantes para respaldar las IICC y SSEE y mantener la seguridad nacional que a continuación se presentan[10]:

[9] https://diario.uach.cl/chile-es-el-cuarto-pais-de-america-latina-con-mas-intentos-de-ciberataques-por-mensajes-fraudulentos/
[10] https://www.cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems

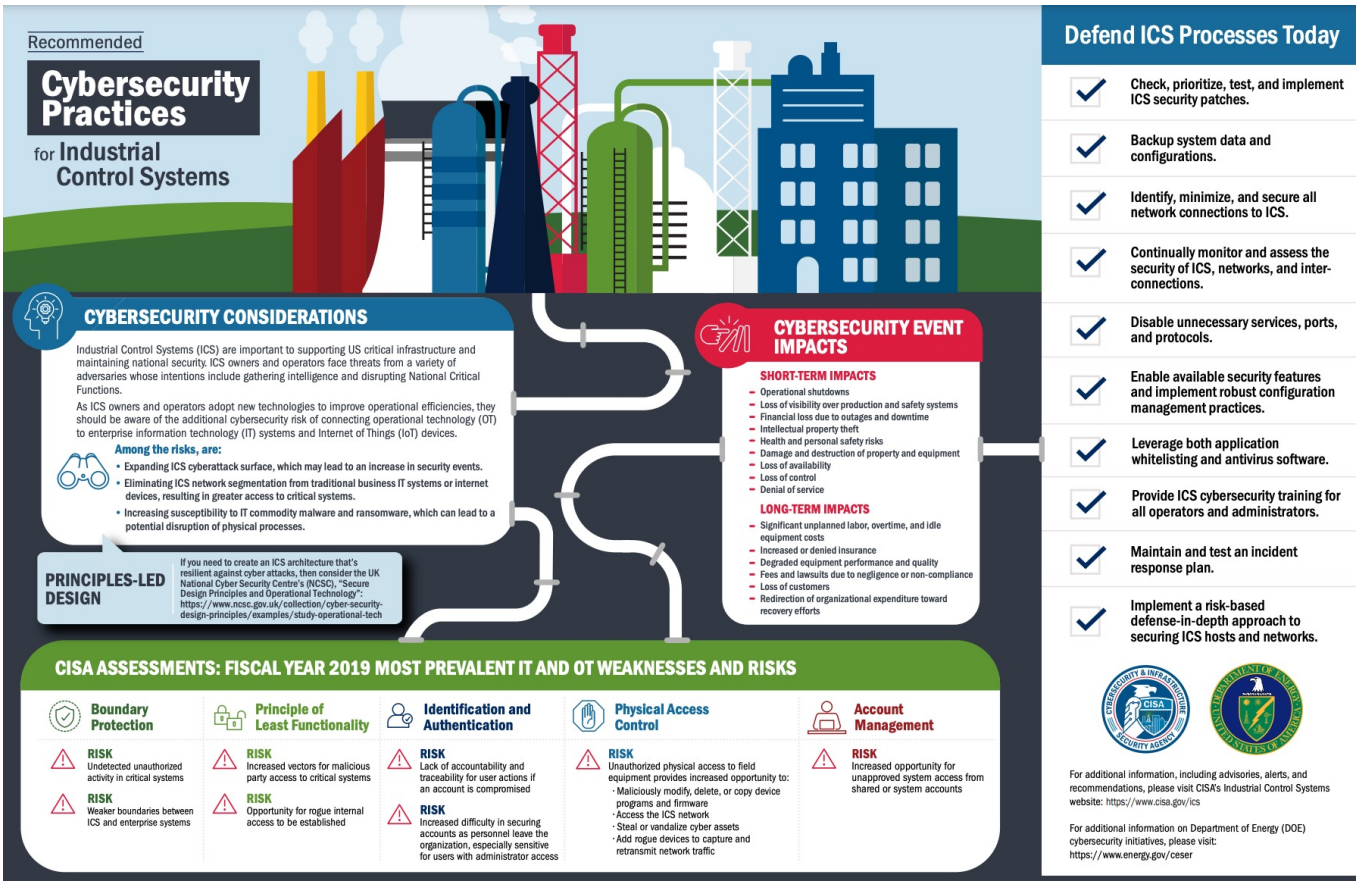


Figura 1: Prácticas de Ciberseguridad para Sistemas de Control Industrial

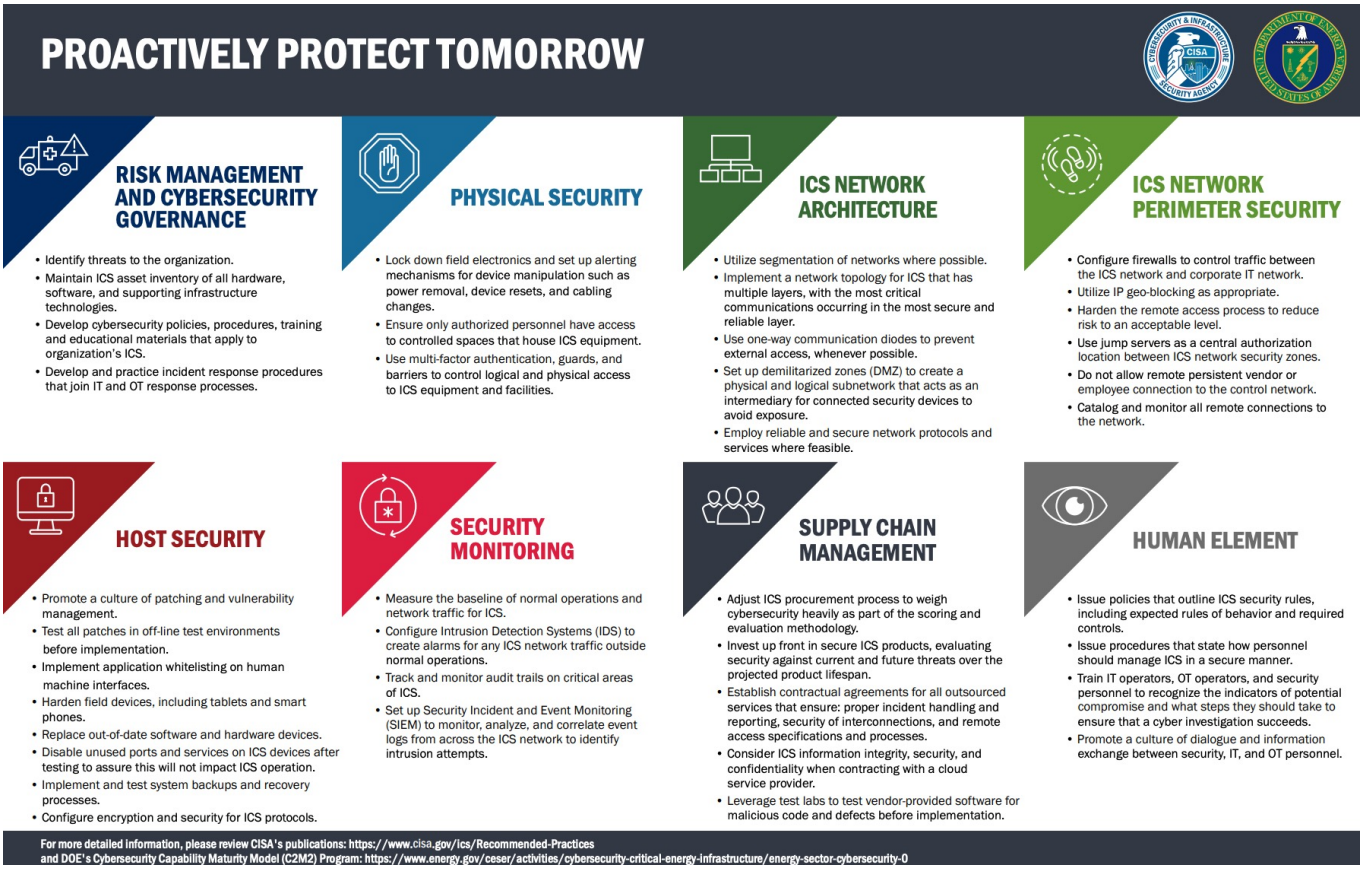


Figura 2: Recomendaciones para Protección de Sistemas de Control Industrial

5. DEFINICIONES Y PROPUESTA DE SECTORES ESTRATÉGICOS

A continuación, se presentan algunas definiciones y propuestas basadas en la Ley Española 8/2011 (28 de abril)[11], por la que se establecen medidas para la protección de las infraestructuras críticas:

*** Servicio esencial (SSEE):** El servicio necesario para el mantenimiento de las funciones sociales básicas, la salud de la población, la seguridad, el bienestar social y desarrollo económico de los ciudadanos, entregado por organismos públicos o privados.

*** Sector estratégico:** Cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva del país, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país.

A continuación, se proponen 14 sectores estratégicos básicos:

- **Energía**
- **Telecomunicaciones**
- **Aguas**
- **Administración Pública**
- **Salud y Servicios de Emergencias**
- **Financiero**
- **Transporte**
- **Industria Crítica**
- **Alimentación**
- **Educación**
- **Instalaciones de Investigación**
- **Organizaciones Tecnológicas**
- **Industria Química**
- **Instalaciones Comerciales**

Y se consideran 2 sectores estratégicos especiales, tanto por su reglamentación especial como por su desarrollo a futuro, respectivamente:

- **Defensa y Seguridad Pública**
- **Espacio**

[11] Disponible en: https://www.boe.es/eli/es/l/2011/04/28/8

*** Infraestructuras críticas:** Son las infraestructuras compuestas por las instalaciones físicas, redes, nubes, sistemas y equipos físicos en los ambientes de: Tecnologías de la Información (TI) y/o Tecnologías de Operación (TO) y/o Sistemas de Control Industrial y/o dispositivos del Internet de las Cosas (IoT/IIoT), sobre las que descansa el funcionamiento de los servicios esenciales, y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

*** Análisis de riesgos:** El estudio de las hipótesis de amenazas posibles necesario para determinar y evaluar las vulnerabilidades existentes en los diferentes sectores estratégicos y las posibles repercusiones de la perturbación o destrucción de las infraestructuras que le dan apoyo. Se presenta usualmente bajo el conecpto de Matriz de Riesgos.

*** Zona crítica:** Aquella zona geográfica continua donde estén establecidas varias infraestructuras críticas a cargo de operadores diferentes e interdependientes, que sea declarada como tal por la Autoridad competente. La declaración de una zona crítica tendrá por objeto facilitar la mejor protección y una mayor coordinación entre los diferentes operadores titulares de infraestructuras críticas (públicas o privadas) radicadas en un sector geográfico reducido, así como con las Fuerzas y Cuerpos de Seguridad del Estado y las Policías de Orden y Seguridad.

*** Criterios de criticidad:** Los parámetros en función de los cuales se determina la criticidad, la gravedad y las consecuencias de la perturbación o destrucción de una infraestructura crítica se evaluarán en función de:

1. El número de personas afectadas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.

2. El impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios.

3. El impacto medioambiental, degradación en el lugar y sus alrededores.

4. El impacto público, reputacional y social, por la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

*** Nivel de Seguridad:** Definido en un Plan Nacional de Protección de Infraestructuras Críticas, de acuerdo con la evaluación general de la amenaza y con la especifica que en cada supuesto se efectúe sobre cada infraestructura, en virtud del cual corresponderá declarar un grado concreto de intervención de los diferentes organismos responsables en materia de seguridad.

*** Interdependencias:** Los efectos que una perturbación en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el propio sector y en otros sectores, y las repercusiones de ámbito local, nacional o internacional.

*** Protección de infraestructuras críticas:** el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia.

*** Información sensible sobre protección de infraestructuras críticas:** los datos específicos sobre infraestructuras críticas que, de revelarse, podrían utilizarse para planear y llevar a cabo acciones cuyo objetivo sea provocar la perturbación o la destrucción de éstas.

*** Operadores críticos u Operadores de Servicios Esenciales:** las entidades u organismos, responsables de las inversiones o del funcionamiento diario de las infraestructuras críticas, tanto públicas como privadas.

*** Organizaciones Tecnológicas:** las empresas que dan soporte y gestión tercerizada a las infraestructuras críticas a nivel de sus sistemas, nubes y redes en los ambientes de: Tecnologías de la Información (TI), y/o Tecnologías de Operación (TO) y/o Sistemas de Control Industrial y/o dispositivos del Internet de las Cosas (IoT/IIoT). (Estos proveedores no son responsables de la seguridad del servicio esencial, pero si deben alertar, informar y reportar de manera oportuna, ante cualquier amenaza de ciberincidente, lo cuál implica que deben tener un sistema robusto de alerta temprana por reglamento ante ciberincidentes de ciberseguridad)

*** Catálogo Nacional de IICC y SSEE :** la información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras críticas existentes en el territorio nacional y que es llevada y manejada en forma reservada actualizada por la Autoridad competente.

6. PRINCIPALES LINEAMIENTOS ESTRATÉGICOS PROPUESTOS

Una futura Política o Estrategia Nacional de IICC y SSEE debiera considerar al menos los siguientes lineamientos estratégicos.

1. CIBER RESILIENCIA. El país debe contar con una infraestructura critica resiliente, tanto física como virtual, preparada para identificar, proteger, detectar, anticipar, responder, mitigar y recuperar ante incidentes de ciberseguridad. Lo anterior bajo un enfoque centrado en la gestión de riesgos, y seguridad de la información

2. CULTURA Y CONCIENCIACIÓN. Es imperativo desarrollar y establecer una Cultura de Protección de nuestras Infraestructuras Críticas y Servicios Esenciales a nivel país, con el fin de generar conciencia en la ciudadanía. Esta cultura debe ser parte de la gestión permanente de cada uno de los operadores críticos de servicios esenciales, mediante la adopción de buenas prácticas, estándares internacionales, capacitación sectorial, acreditación de competencias, y campañas periódicas de responsabilidad tanto individual como colectivas.

3. CSIRT SECTORIALES. Conformar los Equipos de Respuesta ante Incidentes de Seguridad Sectoriales (CSIRTs Sectoriales) conforme a la ley marco en ciberseguridad. Estos deberán estar estrechamente coordinado con el CSIRT Nacional, el que será parte de la Agencia Nacional de Ciberseguridad, con el fin de manejar temas como alertas tempranas, seguimiento y respuesta conjunta a ciberincidentes.

4. GOBERNANZA. una Estructura Organizacional de Protección de Infraestructuras Críticas que vele por la gobernanza y el cumplimiento de los planes y programas de protección sectoriales, así como también por la coordinación, comunicación y planificación ante incidentes de seguridad que comprometan nuestra infraestructura crítica nacional, llevando un Catálogo Nacional de IICC Y SSEE.

5. NORMATIVAS SECTORIALES. Definición y Creación de Planes y Programas Sectoriales Específicos para cada uno de los sectores críticos basados en una Política Nacional de IICC y SSEE Difusión y programas de adopción de normas.

NOTA: los puntos 3,4 y 5 se encuentran abordados en la tramitación de la Ley Marco de Ciberseguridad (Boletín 14.847-06), actualmente en trámite legislativo.

6. CIBEREJERCICIOS. Planificar y participar en Ciberejercicios Nacionales (multisectoriales) e Internacionales que permitan evaluar la ciber-resiliencia de las IICC y SSEE, así como también mejorar la capacidad y aprendizaje de los recursos humanos especialistas de los operadores críticos.

7. MES DE LA IICC. Establecer, al igual que en otros países, el mes nacional de la IICC y SSEE, con el objeto de promover actividades de difusión sobre su importancia, coordinar actividades de simulación y evaluación de efectos de fallos o incidencias multisectoriales.

8. MEDICIÓN DE MADUREZ. Medir anualmente los avances y evolución de la madurez de ciberseguridad de los países de acuerdo a estándares como el Modelo de Madurez de Ciberseguridad para las Naciones (CMM) de Oxford, de tal manera de definir brechas y planes de acción de mejoras en cada sector.

9. GESTIÓN DEL TALENTO. Fomentar la capacitación, educación, innovación y desarrollo de nuevos talentos en Universidades, Organizaciones Públicas y Privadas, Responsables de IICC. de los operadores críticos, entre otros, a través de un Instituto Nacional de Ciberseguridad con alianzas internacionales y nacionales para el desarrollo de capacidades para la protección de IICC y SSEE.

10. ALIANZAS Y COOPERACIÓN. Crear y fomentar vínculos nacionales e internacionales de alianzas y cooperación con organismos gubernamentales, centros de investigación, universidades, equipos de respuesta a incidentes cibernéticos, entre otros, que permitan la transferencia de conocimiento, capacitación y certificaciones, tanto globales como sectoriales, en lo que respecta a la protección de IICC. aumentando así las capacidades de defensa nacional.

7. INICIATIVAS PROPUESTAS

Proponer una Hoja de Ruta en materia de Protección de IICC, permite alinear los esfuerzos transversales y multisectoriales con respecto al tema. En una perspectiva de corto, mediano y largo plazo reflejando así el sentido de urgencia en su implementación.

Con una mirada holística, se proponen un conjunto de inciativas, algunas transversales que trascienden las ICC y otras más acotadas que responden a sectores estratégicos específicos.

Estas iniciativas se enmarcan en cada uno de los 9 lineamientos estratégicos propuestos para la Protección de IICC y SSEE. Las iniciativas marcadas con (*) se consideran de alta prioridad estratégica:

1) GOBERNANZA

Acciones a corto plazo

→ Establecimiento de una Política Nacional de Ciberprotección a las IICC y SSEE
→ Creación de Agencia Nacional de Ciberseguridad
→ Creación del CSIRT Nacional dependiente de la Agencia Nacional de Seguridad
→ Creación de la Agencia Nacional de Protección de Datos Personales.
→ Obligación de reportar aquellos incidentes que generen compromisos sobre las IICC y/o SSEE que tengan un impacto en la población.
→ Establecimiento de un marco legal sancionatorio para quienes ataquen por medios digitales IICC o SSEE, así como a los responsables en acciones negligentes (deliberadas o por omisión) dentro de la generación de ciberataques dentro de las instituciones.

Acciones a mediano plazo

→ (*) Creación de un Centro Nacional de Protección de IICC o entidad a fin.
→ Operadores de IICC y SSEE deben implementar SGSI (Sistemas de Gestión de Seguridad de la Información), que consideren la Ciberseguridad Industrial en todos sus procesos críticos.
→ Para la Seguridad Industrial en los operadores esenciales, el alineamiento con estándares reconocidos internacionalmente, como por ejemplo el IEC62443 (Security For Industrial Automation And Control Systems), como línea de base para diseños seguros.
→ Creación de un Instituto Nacional de Ciberseguridad con el propósito de promover la ciberseguridad, orientar la investigación y el desarrollo de talento humano en materia de ciberseguridad.

Acciones de Largo Plazo

→ Establecimiento de una Oficina Nacional de Ciberseguridad y Ciberdefensa (similar a Senapred) a objeto de coordinar las respuestas a incidentes que afecten a nivel país por causa de cibertaques a IICC y SSEE.

2) CIBER RESILIENCIA

Acciones a corto plazo

→ Confección y difusión de Metodología Risk Assesment (Evaluación de Riesgos) con énfasis en Protección de IICC y SSEE, bajo supervisión de la Agencia Nacional de Ciberseguridad en colaboración con los principales expertos en la materia, alineado a una Política Nacional de Protección de IICC y SSEEE.

Acciones a mediano plazo

→ Establecer un catálogo nacional de IICC y SSEE conforme a criterios y normas establecidos por la autoridad competente, de manera que ésta pueda establecer mapas de interdependencia (manejo del efecto Dominó). Hacer exigible los planes de Gestión y Respuestas de Incidentes de Ciberseguridad.

Acciones de Largo Plazo

→ Plan automatizado de evaluación de Riesgos e Impactos cibernéticos basados en herramientas de IA (Inteligencia Artificial) que permitan mejorar la toma de decisiones frente a distintos escenarios que puedan derivarse de un ciberataque.

3) NORMATIVAS SECTORIALES

Acciones a corto plazo

→ Promulgación de normativas, guías y directivas de mejores prácticas sectoriales, liderado por la Agencia Nacional de Ciberseguridad.
→ Obligación, para todas las IICC y SSEE, de contar con un responsable de Ciberseguridad registrado (CISO) y que sea éste quien se relacione con la Agencia Nacional de Ciberseguridad y Csirt Sectoriales. Establecer un registro nacional de responsables .
→ Establecimiento de marcos sancionatorios por incumplimientos normativos en materias de ciberseguridad

Acciones a mediano plazo

→ Establecimiento de planes y programas sectoriales de ciberseguridad alineados con una Política Nacional de IICC y SSEE.
→ Establecimiento de certificaciones estandarizadas en materia de cumplimiento normativo.

Acciones de Largo Plazo

→ Establecimiento de reglamentos y normas sectoriales de Protección de IIC y SSEE (tanto en Ciberseguridad como Protección de Datos), a cargo de la Agencia Nacional de Ciberseguridad.

4) CSIRTS SECTORIALES

Acciones a corto plazo

→ Planificación Estratégica (Presupuesto, Diseño, Dotación, Entrenamiento) de los CSIRTS sectoriales que se definan, con apoyo de la Agencia Nacional de Ciberseguridad a través del CSIRT Nacional.

Acciones a mediano plazo

→ (*) Conformación de CSIRTS Estratégicos.
→ Los sectores estratégicos que no puedan contar con un CSIRT sectorial propio, se subordinarán al CSIRT Nacional.

5) ALIANZAS Y COOPERACIÓN

Acciones a corto plazo

→ Establecer alianzas de colaboración entre los sectores estratégicos con el CSIRT nacional, CSIRT de Defensa, Policía de Investigaciones y Cibercrimen, así como centros de Investigación en ciberseguridad y ciberinteligencia.
→ Fomentar alianzas de cooperación público-privadas para apoyar la elaboración políticas de resguardo de la seguridad digital de las IICC y SSEE interdependientes.

Acciones a mediano plazo

→ Alianzas y cooperación de CSIRTS sectoriales, con centros de Protección de IICC tanto regionales como otros referentes internacionales (España, Estonia, Reino Unido, USA).

Acciones de Largo Plazo

→ Alianzas y Cooperación con CSIRT Nacional y CSIRT de Defensa para establecer elementos de Protección ante escenarios de ciberguerra .

6) CIBEREJERCICIOS

Acciones a corto plazo

→ Programar Ejercicios Nacionales de Ciberseguridad en los sectores públicos, privados, academia, y defensa, que consideren blancos objetivos las IICC y SSEE para mejorar las capacidades humanas y mejora de la resiliencia.

Acciones a mediano plazo

→ Ciberejercicios Internacionales con Aliados Regionales

Acciones de Largo Plazo

→ Ciberejercicios Internacionales con organismos y aliados internacionales.

7) MEDICIÓN DE MADUREZ

Acciones a corto plazo

→ Medición de Niveles de Madurez en Ciberseguridad para medir brechas iniciales y definir Índices de claves de desempeño (KPI), bajo el liderazgo de la Agencia Nacional de Ciberseguridad.

Acciones a mediano plazo

→ (*) Medición Anual de los niveles de Madurez en Ciberseguridad de acuerdo al Modelos de la Universidad de Oxford (CMM), y generar acciones tendientes a mejorar los índices de desempeño y reducir las brechas.

Acciones de Largo Plazo

→ (*) Seguimiento permanente de los índices de gestión sectoriales para mantener y mejorar la madurez en ciberseguridad

8) GESTIÓN DEL TALENTO

Acciones a corto plazo

→ Creación y difusión de Plan de estudios para operadores de IICC y SSEE como línea de base, inspirados en programas similares como el SANS Institute, National Initiative for Cybersecurity Education (NICE) entre otros, apoyados por la Agencia Nacional de CibesSeguridad y el Instituto Nacional de Ciberseguridad a ser creados.

Acciones a mediano plazo

→ Coordinación a través del Instituto Nacional de Ciberseguridad para establecimiento de programas formativos para carreras, especializaciones, diplomados y afines en materias de Ciberseguridad, incluidos Magister en Protección de IICC.
→ Establecimiento de certificaciones y homologaciones reconocidas para los especialistas en Ciberseguridad (procesos de acreditación).

Acciones de Largo Plazo

→ Establecimiento de actividades de I+D+i en productos y soluciones de Ciberseguridad, protección de datos personales y, ciberinteligencia como un polo de desarrollo nacional.

9) CULTURA Y CONCIENCIACIÓN

Acciones a corto plazo

→ Proyecto de Ley que declara Noviembre como mes Nacional de las IICC y SSEE, en el mes de noviembre complementando el mes de la Ciberseguridad.

Acciones a mediano plazo

→ Educación y creación de conciencia sobre ciberseguridad a edades tempranas, con énfasis en la ciberhigiene para el adecuado comportamiento y protección de datos en el ciberespacio, con énfasis en el cuidado de nuestras IICC y SSEE.

Acciones de Largo Plazo

→ Acciones permanentes de promoción de la ciberseguridad como campañas focalizadas hacia lo público y privado, así como al interior de organizaciones relacionadas con la protección de nuestras IICC y SEE

Por su parte, a continuación, se proponen algunas otras iniciativas sectoriales que refuerzan la protección de IICC y SSEE, reconociendo que industrias como la banca y las telecomunicaciones, están fuertemente reguladas por sus autoridades sectoriales en materias de ciberseguridad.

Por ello y por el cual sólo, a modo de referencia, se presentan iniciativas sectoriales en los sectores de: Aguas e Industria Crítica, que servirán de referencia a otros sectores que deban a futuro seguir profundizando su nivel de madurez en ciberseguridad.

Iniciativas sectoriales tácticas operacionales para el Sector de Aguas

1) Gobernanza

Acciones a corto plazo

→Contar con Oficiales de Ciberseguridad con competencia y acreditación

Acciones de Mediano Plazo

→Diseño de políticas, roles y perfiles de accesos a entornos OT-IoT-IIoT

Acciones de Largo Plazo

→Evalaución y plan de tratamientos de riesgos en ciberseguridad industrial

2) Ciber Resiliencia

Acciones a corto plazo

→Securitizacion y políticas de hardening de computadores de operación OT-IoT-IIoT
→Gestión de usuarios privilegiados
→Implementar controles de protección de perímetro

Acciones de Mediano Plazo

→Securitizacion y Políticas de Hardening de Computadores de operación OT-IoT-IIoT
→Gestión de usuarios privilegiados
→Aplicar Segregación de entornos OT-IoT-IIoT

Acciones de Largo Plazo

→Aplicación de controles sobre periféricos (Bloqueo USB, solidificación de computadores de operación) como alternativas
→Directorio activo dedicado para entorno OT-IoT-IioT

3) Normativas sectoriales

Acciones a corto plazo y mediano plazo

→ISA 95 - ISO 27001

Acciones de Largo Plazo

→IEC 62443

4) CSIRT Sectoriales

Acciones de Mediano Plazo

→Establecer CSIRT sectorial para la industria de las Aguas

5) Alianzas y Cooperación

Acciones de Mediano Plazo

→Organizaciones del mismo sector. Coordinación con CSIRT Nacional

6) Ciberejercicios

Acciones de Mediano Plazo

→Desarrollar planes de continuidad de Negocio, Análisis de Impacto Regulatorio (RIA), Análisis de Impacto de Negocios (BIA) para los entornos OT-IoT como parte de la normativa sectorial
Acciones de Largo Plazo
→Generar pruebas de continuidad de entornos (Plan de recuperación de desastres DRP) como parte de la Normativa Sectorial

7) Medición de Madurez

Acciones de Mediano Plazo

→Auditorías y revisión de vulnerabilidades
Acciones de Largo Plazo
→Aplicar herramientas de Ciberinteligencia

8) Gestión del Talento

Acciones de Mediano Plazo

→Formar equipo de ciberseguridad sectorial respecto de amenazas y vulnerabilidades de ciberseguridad industrial.

9) Cultura y concienciación

Acciones de Corto Plazo

→Generar plan de formación y cibereducación en Ciberseguridad Industrial.
Acciones de Mediano Plazo
→Generar charlas dy capacitación de ciberseguridad industrial a personal de operaciones en entornos OT-IoT-IIOT
Acciones de Largo Plazo
→Evaluación y seguimiento de la eficacia de la cultura y concientización en ciberseguridad industrial

Iniciativas sectoriales tácticas operacionales para el Sector de Industria Crítica

1) Gobernanza

Acciones a corto plazo

→Definición sub-sectores específicos y punto de corte para riesgo alto, medio y bajo de operadores Industria Crítica (por tamaño e impacto potencial a la sociedad y economía)

Acciones de Mediano Plazo

→Definición de mecanismos de interacción de Operadores Industria Crítica con la Agencia Nacional de Ciberseguridad.

Acciones de Largo Plazo

→Definición de mecanismos de interacción de Operadores Industria Crítica con Centro Nacional de Protección de IICC.

2) Ciber Resiliencia

Acciones a corto plazo

→Plan de autoevaluación anual de riesgo de ciberseguridad, en base a pautas predefinidas. Resultado permitirá mantener actualizados niveles de riesgo.

Acciones de Largo Plazo

→Incorporar en plan de pruebas al termino de jornada (COB) de Operadores Esenciales a los Operadores De Industria Crítica de Alto Riesgo

3) Normativas sectoriales

Acciones a mediano plazo

→Establecer normativas y plazos de implementación para operadores de Industria Crítica según nivel de riesgo identificado (alto, medio, bajo)

Acciones de Largo Plazo

→Difundir y capacitar a los operadores de Industria Crítica en las metodologías acordadas. Implementar procesos de revisión periódica de cumplimiento.

4) CSIRT Sectoriales

→No aplica

5) Alianzas y Cooperación

Acciones de Mediano Plazo

→Potenciar cooperación e intercambio de conocimientos (know-how) en ciberseguridad con matrices internacionales o empresas afines, de operadores de Industria Crítica.

6) Ciberejercicios

Acciones de Mediano Plazo

→Incluir a los operadores de Industria crítica en ejercicios sectoriales.

Acciones de Largo Plazo

→Considerar ejercicios con escenarios de fallos catastróficos para la Industria Crítica

7) Medición de Madurez

Acciones de Corto Plazo

→Establecer niveles de madurez en ciberseguridad para operadores de Industria Crítica según los niveles de riesgo del operador, y plazos para llegar al objetivo deseado.a

Acciones de Mediano Plazo y Largo Plazo

→Establecer métrica para medir grados de madurez y plazos para logro de objetivos.

8) Gestión del Talento

Acciones de Corto Plazo

→Establecimiento de requisitos para establecer la necesidad u obligatoriedad de cumplir con un CISO (interno o externo) para los Operadores Críticos de alto riesgo

Acciones de Mediano Plazo

→Extender y Homologar cursos internos realizados por la IICC y SSEE a los operadores de Industrias Críticas.

Acciones de Largo Plazo

→Establecimiento de requisitos para establecer la necesidad u obligatoriedad de cumplir con un CISO (interno o externo) para los Operadores Críticos de mediano y bajo riesgo.

9) Cultura y concienciación

Acciones de Mediano y Largo Plazo

→Establecimiento programas de difusión en ciberseguridad, evaluación y seguimiento de la eficacia de la cultura y concientización en Ciberseguridad.

El conjunto de propuestas considera que existirá una gobernanza en ciberseguridad y servicios esenciales, basada en la legislación que está siendo tramitada en el parlamento, y que considera un impulso a la educación y cultura en ciberseguridad, así como la existencia de una legislación robusta y actualizada en materia de protección de datos.

A su vez, es importante reiterar que un marco regulatorio para la IICC y los SSEE es un aspecto relevante que permite entre otras cosas, la creación de CSIRTs sectoriales, catálogos de IICC, y medición de madurez de la gestión en Ciberseguridad (creando Índices de Desempeño KPI).

8. PRINCIPALES CONCLUSIONES Y RECOMENDACIONES

La Ciberseguridad es un elemento transversal para la transformación digital, y no sólo para un ecosistema que involucra a las empresas y sus stakeholders, sino también para todos los Estados en el mundo. Unos Estados que hoy necesitan defenderse más que nunca de la mala intencionalidad que existe en el ciberespacio y que actualmente está incidiendo reiteradamente en actividades públicas y empresariales (ciberguerra, crimen organizado, hacktivismo y organizaciones criminales) en especial sobre Infraestructuras Críticas de las cuales depende la estabilidad y la operación diaria de su población, (en áreas como Energía, y servicios públicos como Aguas, Telecomunicaciones, Salud, Finanzas y Transporte entre otros).

Se reconoce que la cultura de la ciberseguridad aún es incipiente en Chile, y no logra impregnarse en la Industria, en la economía, legislación actual y ciudadanía de nuestro país. En este escenario, las iniciativas de ciberseguridad, donde existe una estrecha colaboración del mundo público y privado, cobran más valor puesto que ayudan a entender y sumar esfuerzos por impulsar mecanismos e instrumentos necesarios, para garantizar tanto ciberseguridad como resiliencia, frente a disrupciones.

Solo de esta forma se podrá evitar poner en riesgo la integridad y continuidad operacional de nuestras Infraestructuras Críticas y sus servicios esenciales. Dichos instrumentos deben estar basados en un marco legal, normativo y regulatorio, los cuales deberían desembocar en una **Estrategia Nacional de Ciberseguridad**, entendiéndose esta como Política de Estado.

El fin común que deberá tener esta estrategia, es garantizar un uso seguro y fiable del ciberespacio chileno, y así proteger los derechos y libertades de sus ciudadanos, promoviendo además su progreso socioeconómico enfocándose en factores claves como:

1. Protección de la Infraestructura crítica. Se debe promover e impulsar un marco legal que al igual que en otros países, permita la definición de un marco de roles y responsabilidades, públicos y privados, y establezca un conjunto de alertas, notificaciones y respuestas frente a eventos de ciberseguridad asociados a los sectores críticos y esenciales para la ciudadanía.

2. Crear cultura de ciberseguridad a nivel país, involucrando a la Academia, la Industria, el Estado y la sociedad. De acuerdo con el Informe Global de Riesgos 2022, emanado por el Foro Económico Mundial, se asegura que el 95% de los riesgos cibernéticos son productos de fallas humanas.[12] Por esta razón, se hace necesario generar y promover una cultura transversal de ciberseguridad, que aborde los sectores de la Industria, Economía, el aparato público y Academia, ayudando de esta forma a mitigar el riesgo de abrir una posible brecha producto de un error humano.

[12] Disponible en: https://www.marsh.com/co/risks/global-risk.html

3. Crear la Agencia Nacional de Ciberseguridad. A la cual se le deben otorgar los instrumentos necesarios para prevenir y combatir los delitos informáticos que suceden en la red de Internet. "Esta agencia será el órgano que entregue seguridad a los chilenos en el ciberespacio, que proteja los bienes y activos de la sociedad digital, y que se coordine con el sector privado de manera permanente para garantizar la seguridad de los ciudadanos en el ciberespacio"[13]

4. Establecer un marco normativo y regulatorio a nivel sectorial, que establezca deberes y responsabilidades de cada miembro de un determinado sector, entregándoles los lineamientos mínimos requeridos para la prevención, respuesta y resolución de los incidentes de ciberseguridad.

5. Certificación en materia de ciberseguridad, para las Infraestructuras Críticas y Servicios Esenciales. Todas aquellas organizaciones públicas o privadas que sean clasificadas como Infraestructuras Críticas de la Información deberán implementar y mantener un sistema de gestión de riesgo de seguridad de la Información y de continuidad operacional certificados por organizaciones validadas por la industria y la academia.

6. Implementación de CSIRT sectoriales. Estos deben ser capaces de responder ante incidentes de ciberseguridad que puedan poner en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información de sus respectivos sectores regulados,[13] debiendo además reportar y coordinarse con la Agencia Nacional de Ciberseguridad.

7. Apoyo a la academia y a la industria de I+D de Ciberseguridad a nivel nacional. El marco normativo debe establecer los canales que faciliten la firma de convenios entre el sector público, privado, académico e industria I+D de ciberseguridad, esto con la finalidad de establecer una cooperación mutua, transferencia de conocimiento e investigaciones que agreguen valor, vale decir, aportando soluciones específicas para el país.

8. Protección en la cadena de suministro. Ya que la mayor parte de los insumos utilizados para la producción de un bien o servicio, no se manejan de manera interna, para obtenerlos de manera oportuna, las organizaciones dependen de cadenas de suministro altamente integradas a la línea de producción. Por lo tanto, se hace necesario el regular a todos aquellos proveedores de las Infraestructuras Críticas con una serie de medidas y requerimientos tanto de seguridad física como lógica, con el objetivo de prevenir y resolver incidentes cibernéticos, y a la vez mitigar posibles impactos en la continuidad de los servicios.

[12] https://www.csirt.gob.cl/noticias/presidente-pinera-anuncia-proyecto-de-ley-que-crea-la-agencia-nacional-de-ciberseguridad/

[13] https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06

9. Alianzas estratégicas con otros países. Generar las redes de contacto necesarias para reunir a los ámbitos, público, privado y académico, en donde se compartan los intereses y conocimientos en materia de ciberseguridad, se fomente además la educación, el uso responsable de las tecnologías, y los canales de comunicación. Pero esto no solo a nivel nacional, sino traspasando fronteras, ampliando así cada vez más la base del conocimiento.

En definitiva, el esfuerzo mancomunado de todos los sectores y organizaciones tanto privadas como públicas, así como del ejecutivo y legislativo debe converger en el futuro establecimiento de una **Política Nacional de Infraestructuras Críticas,** que establezca las bases sobre la cual nos permita enfrentar los riesgos y amenazas, provienen tanto del mundo físico como digital, y que podrían comprometer el funcionamiento de nuestro país

A modo de resumen, teniendo nuestro país un importante desarrollo de infraestructura tecnológica, adoptando estándares internacionales y con una adecuada base para seguir enfrentando la necesaria Transformación Digital, es relevante trabajar de manera colaborativa en desarrollar las necesarias regulaciones y normativas para mejorar la necesaria protección frente a las amenazas que conllevan los cambios de tecnologías, que van en directo beneficio de nuestra sociedad.

Como propuesta, el presente documento, servirá de importante referente e insumo a los tomadores de decisiones, pues refleja la visión diversa de profesionales y especialistas que han realizado un trabajo desinteresado conjugando múltiples posiciones procurando una propuesta que sea un real aporte a la Ciberseguridad nacional, que permita seguir siendo un referente en el contexto latinoamericano.

*Capítulo 6_*

Estrategia Nacional Contra la Desinformación en Línea

PARTICIPARON EN LA ELABORACIÓN DE ESTE TEXTO:

- Equipo Coordinador submesa "Estrategia Nacional contra la Desinformación en Linea": Jorge Gatica y Felix Staicu

- Comité de Trabajo Técnico de la submesa "Estrategia Nacional contra la Desinformación en Linea" convocado por la Comisión formado por: Ricardo Vásquez, María Paz Ilabaca, Juan Ignacio Nicolossi, Sebastián Carey, Carlos Parker, Jorge Astudillo, Pedro Huichalaf , Victoria Hurtado, y Andrés Barrientos.

1. INTRODUCCIÓN

El aumento explosivo de las tecnologías de la información y la masificación del acceso a ellas, han facilitado las comunicaciones, pero también han impuesto nuevos desafíos. Hoy cada individuo, de manera completamente autónoma, es un potencial generador de contenidos y, dependiendo de la capacidad de cada cual, incluso modelador de la opinión pública.

Hoy los efectos propios de nuestra relación y dependencia del ciberespacio están produciendo cambios relevantes en la sociedad, cuyos efectos apenas comienzan a ser cuantificados en su real magnitud, y conceptos como la cibersociología y cibersicología, aún no están desarrollados a cabalidad para dar respuesta a la magnitud e importancia de estos cambios.

El poder que tiene la información es incuestionable y el mal uso que se puede hacer de ella es un verdadero peligro para las personas y la sociedad en general. Una fotografía, un video o un breve relato bien elaborado y con propósitos definidos, tienen la capacidad de tergiversar dramáticamente una realidad, manipular las mentes, ganar convicciones o destruir la imagen de una institución, organización, figura pública o un ciudadano.

La manipulación del pensamiento individual, grupal o de la sociedad se logra a través de la diseminación de información maliciosamente tergiversada, para obtener réditos políticos, tales como desestabilizar la institucionalidad y subvertir el orden; multiplicadores de fuerza que generan poderosos efectos negativos en la sociedad y en la democracia.

La velocidad, viralidad y anonimato de las redes sociales han exacerbado la polarización partisana, los discursos o incitación al odio, las humillaciones públicas masivas, la intervención extranjera en asuntos internos e informaciones falsas o equivocadas. Cada nueva tecnología de información llega más velozmente y a más personas. La viralidad derivada de algoritmos que amplifican emociones intensas, especialmente la indignación, induce a error, fusionando popularidad con legitimidad; el anonimato, fundamental para la libertad de expresión, ha influido en un diálogo sordo e hiriente que no coopera en el entendimiento de las personas y podría estar afectando gravemente la capacidad de negociación que conlleva toda democracia.

Ante campañas de desinformación avanzadas que explotan las debilidades psicológicas humanas, los notorios algoritmos de las redes sociales y actores que perfeccionan constantemente el arte del engaño, las sociedades son extremadamente vulnerables. La explosión de la información y la habituación

del hombre a la sobrecarga de información han abierto una caja de pandora que ha provocado el declive del pensamiento crítico colectivo. Las defensas tradicionales no funcionan frente a esta amenaza moderna; el primer paso para construir una defensa es comprender la amenaza, para luego contrarrestarla de manera proactiva y reactiva.

Los sistemas de información construidos sobre los cimientos de la democracia y la libertad de expresión se han mostrado vulnerables a las operaciones de influencia externa que utilizan la desinformación como herramienta. La desinformación puede afectar directamente a los cimientos democráticos y, a su vez, las medidas contra la desinformación pueden atentar contra la libertad de expresión. Este es un delicado equilibrio que es necesario tener en cuenta.

Se necesitan herramientas y acciones de diversa naturaleza que permitan abordar sistémicamente desde el diagnóstico hasta la implementación de soluciones. Para lograr lo anterior, se proponen medidas que se pueden clasificar según su enfoque: orientadas a prevenir, reaccionar y orientar la vinculación efectiva entre actores.

No existe un modelo perfecto en la lucha contra la desinformación, ya que es un concepto laxo y dinámico, pero una cosa es cierta: la inacción frente al fenómeno no es una opción por las graves consecuencias sociales que puede implicar. Algunos países, han desarrollado modelos de gobernanza que respetan y refuerzan los procesos democráticos; sin embargo, cada uno está sujeto a críticas y puede mejorarse. Los legisladores deberán aprender de los éxitos y fracasos de otros países y desarrollar un modelo que pueda funcionar y escalarse para contrarrestar las operaciones de influencia, con un horizonte temporal de mediano y largo plazo.

En más de 50 reuniones de trabajo, desarrolladas entre el 22 de junio y el 30 de noviembre de 2022, un equipo conformado por 11 profesionales de formaciones diversas entre los que se cuentan abogados, ingenieros, periodistas, empresarios, académicos y militares, lograron el resultado que se refleja en este capítulo. En el se reúnen conceptos y ejemplos obtenidos de las políticas implementadas por otros países, que han logrado avanzar en el manejo de la desinformación en línea. Un diagnóstico que profundiza sobre un fenómeno que explota las debilidades psicológicas humanas y fisuras sociales, para culminar en la propuesta de una estrategia integral que aborda el problema de forma multidimensional y multisectorial. El propósito final es estructurar una base social, política y cultural sobre la cual se pueda construir una defensa efectiva de la información, fomentando la colaboración entre el sector público-privado.

2. CONTEXTO: EL ALCANCE DEL TÉRMINO DESINFORMACIÓN

La práctica de la desinformación como tal, es una forma aceptada en la batería de instrumentos que un actor posee para el manejo de conflictos, de todos los tipos (bélicos, sociales, individuales, públicos o privados, etc.). Se deriva de la aplicación del principio de engaño al adversario.

En el siglo 5to A.C., el estratega militar Sun Tzu escribía en el capítulo I de su obra "El Arte de la Guerra", que el engaño es la esencia del conflicto y el principio fundamental para la manipulación del adversario.

A lo largo del tiempo, dicho principio se desarrolló sobre la base de la manipulación del pensamiento individual, grupal o social, principalmente asociado en el siglo XX durante la Guerra Fría al área de contrainsurgencia, las que se pusieron en práctica en el sinnúmero de guerras impulsadas por las dos superpotencias hegemónicas de la época.

La metodología esencialmente subversiva y clandestina para la diseminación de desinformación, la que buscaba desestabilizar el orden social en aquellos países donde el adversario estaba radicado, permitió el desarrollo de la teoría moderna de la manipulación de información basadas principalmente en lo que se denomina Operaciones Psicológicas (PSYOPS), arraigadas como uno de los elementos de desestabilización preferidos por los organismos dedicados a las operaciones especiales, muchas veces asociados a los servicios de Inteligencia.

De esta forma, los servicios dedicados a esta función, independiente de su naturaleza militar o civil, implementaron con sutileza procesos de desinformación para alterar la moral y la estabilidad del adversario.

Existe un gran número de tácticas para desinformar, dentro de las cuales se encuentran las variables de malinformación, misinformación y desinformación, los que serán posteriormente definidos. Cabe señalar que la desinformación es una estrategia y las fake news son un tipo de táctica aplicada para generar desinformación, aunque no son las únicas. El arte de la desinformación combina una buena comprensión de la psicología, la sociología, la historia, la política, la economía y otros conceptos relevantes para manipular y propagar astutamente narrativas que influirán en la forma en que las personas y los grupos piensan y toman decisiones.

Si entendemos las tecnologías y el acceso a ellas como multiplicadores de fuerza, lo que encontramos en las tecnologías digitales y sus plataformas, es una relación asimétrica entre los costos de diseminación de información manipulada y su efecto, es decir, una relación económica de bajo costo de implementación con altos niveles de impacto.

del hombre a la sobrecarga de información han abierto una caja de pandora que ha provocado el declive del pensamiento crítico colectivo. Las defensas tradicionales no funcionan frente a esta amenaza moderna; el primer paso para construir una defensa es comprender la amenaza, para luego contrarrestarla de manera proactiva y reactiva.

Los sistemas de información construidos sobre los cimientos de la democracia y la libertad de expresión se han mostrado vulnerables a las operaciones de influencia externa que utilizan la desinformación como herramienta. La desinformación puede afectar directamente a los cimientos democráticos y, a su vez, las medidas contra la desinformación pueden atentar contra la libertad de expresión. Este es un delicado equilibrio que es necesario tener en cuenta.

Se necesitan herramientas y acciones de diversa naturaleza que permitan abordar sistémicamente desde el diagnóstico hasta la implementación de soluciones. Para lograr lo anterior, se proponen medidas que se pueden clasificar según su enfoque: orientadas a prevenir, reaccionar y orientar la vinculación efectiva entre actores.

No existe un modelo perfecto en la lucha contra la desinformación, ya que es un concepto laxo y dinámico, pero una cosa es cierta: la inacción frente al fenómeno no es una opción por las graves consecuencias sociales que puede implicar. Algunos países, han desarrollado modelos de gobernanza que respetan y refuerzan los procesos democráticos; sin embargo, cada uno está sujeto a críticas y puede mejorarse. Los legisladores deberán aprender de los éxitos y fracasos de otros países y desarrollar un modelo que pueda funcionar y escalarse para contrarrestar las operaciones de influencia, con un horizonte temporal de mediano y largo plazo.

En más de 50 reuniones de trabajo, desarrolladas entre el 22 de junio y el 30 de noviembre de 2022, un equipo conformado por 11 profesionales de formaciones diversas entre los que se cuentan abogados, ingenieros, periodistas, empresarios, académicos y militares, lograron el resultado que se refleja en este capítulo. En el se reúnen conceptos y ejemplos obtenidos de las políticas implementadas por otros países, que han logrado avanzar en el manejo de la desinformación en línea. Un diagnóstico que profundiza sobre un fenómeno que explota las debilidades psicológicas humanas y fisuras sociales, para culminar en la propuesta de una estrategia integral que aborda el problema de forma multidimensional y multisectorial. El propósito final es estructurar una base social, política y cultural sobre la cual se pueda construir una defensa efectiva de la información, fomentando la colaboración entre el sector público-privado.

2.1 Desinformación

Con la llegada de las tecnologías de la información, su naturaleza transnacional y su falta de fiscalización, hoy cada individuo o grupo, puede utilizar las prácticas de desinformación a un costo ínfimo, logrando llegar a audiencias masivas en tiempo real. La desinformación se utiliza como herramienta política para influir en elecciones y decisiones políticas, crear inestabilidad y divisiones dentro de la sociedad y actualmente sirve como una herramienta eficaz en el arsenal de cada Estado, grupos influyentes o servicios de inteligencia.

Preparar una ofensiva de desinformación requiere un esfuerzo y recursos relativamente bajos, en comparación con los efectos que genera. Sin embargo, la defensiva es muy complicada de lograr y la mayoría de las veces, las reacciones llegan demasiado tarde para lograr un efecto positivo adecuado y revertir el daño ya causado.

Definir el problema de la desinformación en línea es clave para comenzar a precisar objetivos y desarrollar respuestas. Lo anterior considerando que existen múltiples términos para describir el fenómeno. Por aquello, adoptar definiciones oficiales y usarlas de manera consistente, como propone este capítulo, puede ayudar a institucionalizar los enfoques y asegurarse de que las múltiples causas y manifestaciones de la desinformación en línea, se aborden con precisión.

En ese sentido, es fundamental, en primer lugar, definir el concepto de desinformación en línea y diferenciarlo del popular término fake news. Particularmente, la noción de fake news se hizo mundialmente conocida durante las elecciones presidenciales de los Estados Unidos del año 2016. Allí, su frecuencia como término de búsqueda aumentó significativamente gracias a historias falsas compartidas masivamente a través de redes sociales, llegando a ser nombrada la palabra del año (2017) por el Diccionario Collins.

Aunque no son un fenómeno nuevo y que la información ha sido inventada y manipulada desde tiempos inmemoriales con el objeto de ganar guerras, promover ambiciones políticas, perjudicar a los más vulnerables u obtener lucro económico,[14] no fue hasta el auge de las redes sociales como canal de distribución de noticias, que el concepto volvió con fuerza.

Expertos, autores y organizaciones internacionales han incentivado y recomendado la utilización del concepto desinformación en línea en reemplazo de fake news.[15] Dentro de los argumentos para arribar a dicha

[14] Asamblea General de las Naciones Unidas, La Desinformación y la Libertad de Opinión y de Expresión Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Irene Khan, pág. 2.
[15] Report of the Independent High-Level Group on Fake News and Online Disinformation (European Commission), A Multi-Dimensional Approach to Disinformation, 10.

conclusión, se encuentra principalmente que el concepto de fake news no captura la extensión completa del problema de la desinformación. Particularmente, tiene el problema de ocultar ciertas aristas del fenómeno de la desinformación relacionadas al contenido, formato, motivaciones y agentes involucrados en su distribución (Kalsnes 2018; Wardle and Derakhshan 2017).

Además, el término ha sido utilizado inadecuadamente por diversos actores (especialmente políticos) para desacreditar noticias con las que no están de acuerdo. En efecto, es usado como un genérico para cualquier información en la que la gente no cree (Nielsen and Graves 2017; Waisbord 2018) o para deslegitimar un punto de vista de un opositor (Farkas and Schou 2018). Más aún, el concepto de noticias falsas tampoco es apropiado porque sugiere una dicotomía verdadero/falso en vez de un continuo (Mourao and Robertson 2019,4).

Siguiendo esta línea de ideas, la UNESCO, la OECD, entre otras instituciones[16], han decidido emplear "desinformación en línea" al referirse a este problema. En efecto, la Comisión de la UE adoptó el término desinformación en línea y lo define como "información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población, y que puede causar un perjuicio público[17]". Por perjuicio público se entiende: amenazas a procesos políticos y bienes públicos, incluyendo la protección a la salud, el medio ambiente o la seguridad de los ciudadanos. Igualmente, la OECD, al referirse a la desinformación, la define en función de la acción de "compartir información falsa a sabiendas para causar daño"[18].

Finalmente, leyes y políticas nacionales en diferentes países alrededor del mundo utilizan el concepto desinformación en línea, el cual definen empleando una variedad de elementos distintivos combinados. Estos elementos, incluyen, (i) información falsa o engañosa, (ii) la intención de causar un perjuicio o no, y (iii) la naturaleza del perjuicio causado o buscado[19].

Dentro de los ejemplos concretos es posible encontrar el caso de Estonia, en donde se define a la desinformación en línea como "información falsa o engañosa que se crea y difunde intencionalmente para beneficio político, económico o personal".[20] A su vez, el Reino Unido, en su reporte "daños en línea", la define como información creada o difundida con la intención deliberada de inducir a error; esto podría ser para causar daño o para obtener ganancias personales, políticas o financieras.[21]

[16]Ver, por ejemplo, C. Ireton, y J. Posetti y otros (UNESCO), Periodismo, "Noticias Falsas" & Desinformación Manual de Educación y Capacitación en Periodismo, 6; C. Matasick, C. Alfonsi & otros (OECD), Governance Responses to Disinformation: How Open Government Principles Can Inform Policy Options, OECD Working Papers on Public Governance, No. 39, OECD Publishing, Paris (2020), 12.
[17]European Commission, Communication from the Commission, Tackling Online Disinformation: a European Approach, 3.
[18]OECD, Draft Principles of Good Practice for Public Communication Responses to Mis-and Disinformation, Anexo II (pág. 13).
[19]Asamblea General de las Naciones Unidas, La Desinformación y la Libertad de Opinión y de Expresión Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Irene Khan, pág. 3.
[20]Tyler McBrien, Defending the Vote: Estonia Creates a Network to Combat Disinformation, 2016–2020, Princeton University, pág. 3.
[21]Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department (UK), Online Harms White Paper, pág. 22

Considerando todo lo anterior, para los efectos de la Estrategia que se presenta en este informe, se define a la desinformación como:

"Información deliberadamente manipulada, que es elaborada y/o difundida con el potencial tanto de engañar, como de obtener beneficios y/o causar perjuicio público o privado."[22]

2.2 Conceptos asociados

Otros conceptos asociados a la desinformación en línea se tratan a continuación. Estos son importantes de comprender en cuanto a sus particularidades y diferencias debido a que pueden cambiar significativamente la naturaleza de la amenaza.

2.2.1 Misinformación (induce a error):

Por regla general, por misinformación o información engañosa se entiende aquella información falsa, pero que es creada y/o compartida sin ánimo o intención de generar algún perjuicio o daño. A modo de ejemplo, la Comisión Europea la define como información con contenidos falsos o engañosos compartida, sin intención de perjudicar, aunque sus efectos pueden ser nocivos, es decir, cuando la gente comparte información falsa con amigos y familia, de buena fe.[23]

2.2.2 Malinformación (sabotea):

Respecto a malinformación, su definición tiene por objeto captar la información que se basa en hechos reales, pero que se usa fuera de contexto para engañar, dañar o manipular. Al respecto, la OECD la define como compartir información genuina para causar daño, a menudo moviendo a la esfera pública lo que fue diseñado para permanecer en privado.[24] Esto ocurre, por ejemplo, en el caso de fugas de información.

2.2.3 Operaciones de Influencia:

Este concepto comprende los esfuerzos coordinados de actores nacionales y/o extranjeros, o ambos conjuntamente, para influir en un público destinatario usando una serie de medios engañosos, como la supresión de fuentes de información independientes, unida a la desinformación.

Las operaciones de influencia consisten en redes sofisticadas que propagan información manipulada, para influir en los resultados de un proceso colectivo de toma de decisiones o en el sentimiento público en general. Rara vez se limitan a un medio, por lo general se distribuyen en diferentes plataformas, incluidas las fuentes fuera de línea.

[22] Algunas notas aclaratorias: aunque su difusión es digital, su origen podría estar en otras fuentes de distinta naturaleza (por ejemplo, un comentario de un político); no serán consideradas dentro de la noción de desinformación en línea la publicidad engañosa, los errores de información, la sátira y la parodia; entre los objetivos pueden estar causar un perjuicio público como amenazar procesos políticos, afectar la salud, el medio ambiente o la seguridad de la ciudadanía; cuando se difunde por medios digitales toma el nombre de "desinformación en línea"

[23] Comisión Europea, Plan de Acción para la Democracia Europea, pág. 22.

[24] OECD, Draft Principles of Good Practice for Public Communication Responses to Mis-and Disinformation, Anexo II, pág. 13.

Históricamente, las operaciones de influencia se han manifestado de diferentes formas: desde campañas encubiertas que se basan en identidades falsas hasta esfuerzos mediáticos abiertos y controlados por el Estado que utilizan voces auténticas e influyentes para promover mensajes que pueden o no ser falsos. Sin embargo, cuando un actor oculta su identidad a través de un comportamiento engañoso, el público carecerá de señales suficientes para juzgar quiénes son, qué tan confiable es su contenido o cuál podría ser su motivación.

Es importante separar la desinformación de las operaciones de influencia porque ambas tienen particularidades, impactos y soluciones diferentes al problema. Como parte de una posible solución en este documento, la comunicación con la plataforma de redes sociales es esencial para poder limitar de manera oportuna los efectos del comportamiento malicioso identificado en sus plataformas. Así, entender las diferencias y hablar el mismo lenguaje, en cuanto a la nomenclatura de fenómenos, es esencial para un resultado productivo.

2.2.4. Injerencia extranjera en el espacio de información:

La interferencia extranjera puede tomar la forma de actores externos que buscan manipular la política interna, incluso a través de medios encubiertos y engañosos, para socavar la soberanía política y dañar la cohesión social. En los últimos tiempos, la amenaza de interferencia extranjera ha aumentado en potencial y gravedad debido a Internet y las redes sociales. Estas plataformas han contribuido a la creciente facilidad, sofisticación e impunidad con la que los actores extranjeros hostiles pueden llevar a cabo operaciones de influencia.

Esta idea engloba los esfuerzos coercitivos y engañosos para perturbar la libre formación y manifestación de la voluntad política de las personas por parte de un actor estatal extranjero o de sus agentes. Por regla general, son realizadas como parte de una operación híbrida más amplia (ej. ciberguerra).

2.3 Desinformación al largo plazo (2035)

La desinformación, en tanto amenaza moderna, está recién en una etapa primaria. Las redes sociales comenzaron a ganar fuerza hace solo unos 15 años. El ecosistema de la información es cada día más complejo debido a la explosión de información de la que se rodea el usuario. Recientemente se han desarrollado tecnologías de inteligencia artificial (IA) que están entrenadas para generar contenido escrito con objetivos de manipulación.

La propagación de contenidos en las redes sociales la realizan en su mayoría redes de bots controladas a su vez por algoritmos de IA, que entienden mejor que los humanos las particularidades de los algoritmos de las redes sociales. El aspecto más preocupante, sin embargo, es la mejora de la tecnología deep fake que utiliza IA, a través de redes neuronales GAN (redes generativas antagónicas) para generar contenido de video que imita de manera extremadamente realista la apariencia y la voz de personas reales, siendo el resultado imperceptible para una persona no entrenada o el ojo humano.

En otros 15 años, la peligrosidad en el espacio de la información alcanzará niveles preocupantes y las estrategias actuales probablemente serán obsoletas e ineficaces. Este campo, que se encuentra en una dinámica continua, similar a la ciberseguridad, abrirá las puertas a algunas amenazas que, descontroladas, pueden poner en una situación de extrema peligrosidad los cimientos de la democracia, el estado de derecho y los derechos humanos de cada estado. Ignorar la amenaza no hará que este problema desaparezca, solo creará las condiciones para efectos más dolorosos.

3. LA SITUACIÓN ACTUAL EN CHILE

Realizado un análisis exhaustivo de los problemas actuales de desinformación en Chile, los hallazgos se estructuran en tres subcapítulos que darán origen a los ejes de acción de la estrategia:

- Institucionalidad

- Educación

- Defensa

La estrategia asume los problemas identificados y sugiere una hoja de ruta de soluciones que pueden implementarse para mitigar los problemas identificados.

3.1 Institucionalidad

3.1.1 Marco Normativo

La actual falta de regulación en Chile fomenta un crecimiento sistemático de la desinformación, sin que se imponga ningún límite. La inexistencia de un marco normativo que dicte derechos, obligaciones y responsabilidades en una arquitectura sostenible está creando un ambiente donde no se definen reglas ni responsabilidades de actuación, dejando un vacío descontrolado que genera más problemas.

Una relación no regulada con las empresas de redes sociales está obstaculizando los esfuerzos de las instituciones relevantes para limitar las campañas de desinformación. En países con una legislación más avanzada en la materia, se imponen reglas para las empresas de redes sociales y se establecen canales directos de comunicación con ellas.

3.1.2. Carencia de institucionalidad responsable

En Chile, aun no existe una aproximación institucional organizada para enfrentar los riesgos, implementar medidas normativas, fiscalizadoras y sancionatorias, y que tengan capacidad de establecer procesos de contramedidas para la verificación de información expedita, ya sea ésta establecida vía medios digitales, o clásicos.

La delimitación de responsabilidades es de suma importancia cuando se trata de enfrentar el fenómeno de la desinformación a nivel estatal. Al no existir definiciones claras ni métrica asociada, tampoco se puede ejecutar una respuesta adecuada. Cuando se trata de desinformación, la oportunidad se presenta en tiempos acotados, y ella es fundamental para lanzar una respuesta eficiente, ya que la propagación de la misma se hace muy rápido.

Al ser un fenómeno que afecta trasversalmente a todo el tejido social y, en consecuencia, ser muchos los organismos del Estado y de la sociedad civil vinculados con él, la carencia de una definición normativa en cuanto a tareas y responsabilidades es una falencia relevante.

Por otra parte, la comunicación estratégica es vital para que el Estado se comunique eficientemente con la sociedad civil. El Estado necesita responder de manera efectiva a las campañas de desinformación y tener una estrategia de comunicación preparada, con acciones establecidas para actuar en casos de contingencia.

Esto requiere un organismo responsable del más alto nivel político, destinado a centralizar el esfuerzo en esta materia, sin llegar a constituirse en un censor o una suerte de "ministerio de propaganda", tan lesivo para la democracia y la institucionalidad como ha sido posible observar en varias instancias de la historia mundial.

Al respecto, hay experiencias exitosas que pueden servir como referentes, tales como Francia y Suecia, donde este tipo de organismo se dedica a aspectos relacionados con la educación, la legislación y la defensa, teniendo mecanismos de control para evitar que genere inestabilidad institucional o desbalances democráticos.

3.1.3 Insuficiente capacidad operativa

En el aspecto operativo, la falta de capacidades de análisis y respuesta al tipo de amenazas dinámicas utilizadas por diferentes tipos de actores es evidente. La mayoría de los tomadores de decisión actualmente no comprenden el alcance completo de la amenaza híbrida y no están preparados para responder en caso de que ocurra una crisis. En esta situación, tiempo, procesos, roles y responsabilidades son fundamentales y tienen que ser explícitos y entrenados por todos los actores involucrados, para alcanzar una respuesta eficiente.

Sin un entorno tecnológico y operativo que pueda detectar y comprender adecuadamente la propagación de amenazas de información, las campañas de desinformación son detectadas demasiado tarde o, incluso, pasan desapercibidas y sus efectos pueden ser graves, duraderos o difíciles de revertir.

Un enfoque sistémico es vital para lograr la debida sinergia, evitar superposiciones o áreas grises y alcanzar eficiencia y eficacia. Este es un requisito para lograr un enfoque moderno que permita proteger los intereses de la sociedad chilena en materias de desinformación.

3.2 Educación

3.2.1 Pensamiento crítico

El pensamiento crítico es fundamental en la lucha contra la desinformación, en tanto permite al individuo discriminar entre lo verdadero y lo falso, y adoptar sus propias decisiones. Los países más resilientes a esta anomalía, como Finlandia, han introducido el pensamiento crítico como parte integral de su currículo educativo desde temprana edad, lo que no se ha logrado en Chile. Como indica Jorge Gatica, haciendo referencia a un estudio hecho por la Universidad de Chile "un 44% de los chilenos no entiende lo que lee; más aún, un 80% de la población adulta se encuentra en los dos niveles más bajos de las competencias básicas asociadas a la alfabetización en prosa, en documentos y cuantitativa". [25]

3.2.2 Capacitación sobre desinformación

La falta de conocimiento de la población en general sobre las técnicas de desinformación y las posibilidades de detectarla está creando un entorno en el que la mayoría de las personas no comprenden realmente el espectro de la amenaza y cómo pueden construir una defensa personal resistente contra ella. Faltan campañas de concientización, tanto focalizadas como generales, que puedan introducir y capacitar a la población para detectar información manipulada y denunciarla a las instituciones adecuadas.

[25] Gatica, Jorge. (2016). El enfoque curricular por competencias y la necesidad de innovar en la docencia. En Revista Educación del Ejército de Chile N 43. p. 107

La cultura de la información es un tema muy importante para el futuro del país. Una cultura de ***no compartir antes de verificar*** es fundamental para limitar la difusión de desinformación entre grupos sociales. Los educadores no están capacitados para educar a sus alumnos sobre el tema; además, no tienen acceso a herramientas y materiales para desarrollar en ellos la intuición, actitud y predisposición a filtrar, antes de difundir.

3.2.3 Investigación avanzada

La investigación sobre el tema presenta un nulo desarrollo académico y las instituciones de educación superior en Chile no se están empleando lo suficiente para incentivarla. Esta carencia en investigación de frontera sobre el fenómeno, resulta fundamental; no es posible solo replicar el conocimiento logrado en otros países, ya que la idiosincrasia es una característica relevante y tiene impacto en la forma de operar de quienes utilizan la desinformación y, consecuentemente, en las medidas preventivas y remediales que se adoptan.

3.3 Defensa

3.3.1 Doctrina

En el entorno actual, el uso de la información con fines de influir en las operaciones militares, juega un papel muy importante; aunque siempre lo fue, el alcance que hoy posee a partir de la masificación de las tecnologías de información y comunicaciones, le otorga una connotación muy especial.

El constante desarrollo de mecanismos híbridos de guerra, por debajo del umbral de un conflicto armado, plantea un nuevo escenario de amenazas para Chile. Se requiere que las FF.AA. y de Orden y Seguridad, mantengan capacidades para enfrentar estas nuevas dimensiones del conflicto, las que pueden servir como potenciadoras de una fuerza militar en operaciones convencionales, pero también actuar como una variable independiente en operaciones militares distintas a la guerra.

Por otra parte, resulta fundamental actualizar la doctrina de las FF.AA. y de Orden y Seguridad, de forma tal de darle coherencia a esta con los esfuerzos que se implementarán en estas materias, por parte de otros organismos del Estado y de la sociedad civil.

3.3.2 Capacidad reactiva y proactiva

Las operaciones de influencia e injerencia extranjera representan uno de los mayores peligros para la estabilidad de la democracia chilena. En la etapa actual, la responsabilidad de responder a una amenaza informativa no se comprende adecuadamente, debido a la carencia de normativa, conocimientos y comprensión del fenómeno.

Las instituciones tampoco cuentan con un organismo responsable que esté capacitado para responder al tipo de amenazas presentadas en este documento. Los organismos que se ocuparán de las operaciones de influencia deben tener la capacidad no solo de reaccionar frente a un ataque, sino también de defenderse proactivamente, en línea con el desarrollo de una Estrategia de Ciberdefensa Activa.

Al igual que con la ciberseguridad, se está empleando un enfoque reactivo después de que el daño ya está hecho, con el fin de preparar la defensa para los tipos de amenazas que se desarrollarán constantemente. Sin capacidades ofensivas, los organismos están condenados al fracaso contra actores que emplean ataques avanzados, ya que la realidad actual muestra que la mayoría de los estados (como EE. UU., Francia, Reino Unido o Australia) están empleando la estrategia de defensa cibernética activa para defender sus activos críticos y neutralizar las amenazas.

4. ACTORES INVOLUCRADOS

4.1 Actores estatales

Este fenómeno ha tomado el carácter de riesgo para el Estado de Derecho, la Democracia y los Derechos Humanos; dado este escenario, el Estado debe hacerse cargo y tomar medidas para proteger la institucionalidad y también a los ciudadanos.

Recogiendo las ideas de varios pensadores desde la antigüedad, Maritain indicaba hace casi un siglo que el Estado posee tres tareas fundamentales: el mantenimiento de la ley; el fomento del bienestar común y el orden público; y la administración de los asuntos públicos.

En consecuencia, el Estado tiene un rol insoslayable al momento de enfrentar esta nueva amenaza. Debe ser capaz de crear un marco conceptual, a objeto de armonizar los esfuerzos de los sectores público y privado, las organizaciones del Estado y la sociedad civil, la academia, la ciudadanía en general.

Para estos efectos, hay que generar una institucionalidad adecuada, con organismos especializados y normas específicas. Asimismo, se requiere impulsar la educación destinada a producir el cambio cultural colectivo e individual y también la capacidad proactiva y reactiva para enfrentar agresiones que pudieran provenir en esta área, afectando al país y a cada ciudadano.

Así como la desinformación es relevante para los asuntos internos del país, también lo es para los asuntos externos. Hoy en día la desinformación es utilizada por actores estatales como una herramienta de bajo costo y eficaz para influir en los asuntos internos o externos de otros países. Los conflictos actuales demuestran que una gran parte del conflicto se lleva a cabo en el mundo virtual, empleando un conjunto de técnicas para debilitar a los países e infundir reflejos sociales que favorecen a los atacantes.

4.2 Actores no estatales y redes sociales

Los actores no estatales se están volviendo cada vez más importantes en el espacio de la información. Si hace unas décadas solo el Estado tenían el poder de controlar y manipular la información, hoy todos pueden hacerlo. Es cierto que algunos estados, especialmente aquellos con gobiernos totalitarios o poco democráticos, todavía tienen una preeminencia en lo que respecta a la gestión de la información; pero en las últimas tres décadas, dada la expansión cualitativa y cuantitativa de Internet, cada vez más actores no estatales tienen la posibilidad de influir en el espacio de la información.

El problema no solo se circunscribe a las empresas de redes sociales o medios de comunicación social, sino también a las ONG, los lobbystas, los movimientos sociales, los grupos terroristas y cibercriminales, las grandes corporaciones y muchos otros actores, que utilizan estas plataformas para propaganda u otras acciones antisociales.

El asunto es que, mientras para la acción del Estado existen regulaciones internacionales e internas que rige su comportamiento, los actores no estatales pueden operar con mayor libertad debido a la carencia de normas, a la facilidad para evadirlas o, simplemente a la impunidad (efectiva o perceptiva) ante la falta. A esto coopera significativamente el hecho que la atribución es cada vez más difícil de probar.

En el contexto de mantener el espacio de información libre de interferencias y acciones maliciosas, es necesario dedicar especial preocupación a las empresas de redes sociales. Las principales que están operando en Chile, tienen su sede en el extranjero; por ello, aunque tienen un gran impacto en la calidad de la información con la que interac-

-túa la población chilena, actualmente no existe una forma de comunicarse directamente con ellas ni una regulación que los incentive a retirar material conflictivo.

Como ya se indicó, las empresas de redes sociales sirven como plataforma para actores estatales y no estatales que utilizan el poder de la información digital con fines propios, especialmente de tipo político. Podría ser responsabilidad de estas plataformas limitar la desinformación en sus espacios, pero la mayoría de las veces carecen de suficiente personal y experiencia para detectar cada intento de desinformación.

Por otra parte, ¿son ellas las llamadas a ejercer un acto de censura? ¿Pueden, usando su propio criterio y cánones éticos, limitar la liberta de expresión de un ciudadano?

Recientemente, las plataformas de redes sociales mejoraron sus capacidades de detección de bots, por lo que las grandes operaciones de comportamiento inauténtico coordinado son menos improbables que antes, pero aún posibles.

El campo en el cual las empresas de redes sociales poseen mayores carencias, es en el de las operaciones de influencia. Descritas anteriormente, estas operaciones están estructuradas detalladamente y son muy difíciles de detectar para un observador inexperto o que no entiende las particularidades de un país o su idiosincrasia.

Un analista de informaciones extranjero, sin el debido entrenamiento, conocimiento y experiencia, difícilmente entenderá la cultura de la sociedad chilena, por lo que le será muy difícil detectar y entender cuando se producen operaciones de influencia.

Es por esto que en países avanzados, donde la desinformación se trata con seriedad, las agencias locales dedicadas a este fenómeno complementan el trabajo de los departamentos de Trust and Safety de las empresas de redes sociales y son capaces de alertar sobre operaciones sospechosas cuando estas ocurren; esto permite a las empresas lograr una mayor eficiencia para neutralizar contenidos cuestionables. Para incentivar a las empresas de redes sociales a colaborar en estos temas, una regulación adecuada que les defina sus responsabilidades y obligaciones, debe ser la base para una cooperación eficiente.

Finalmente, es necesario recordar que existe una gran cantidad de otros actores no estatales relevantes que operan en el espacio de la información. Lamentablemente, es muy difícil de regular su accionar, por lo que se requiere generar cambios culturales de forma de alcanzar una

ética que lleve a la autoregulación de organizaciones y personas, lo que implica una robusta colaboración entre todos los actores para lograr un espacio de información saludable, aislando a los agentes antisociales y garantizando un proceso transparente de lucha contra la desinformación.

La colaboración con la sociedad civil es vital para un espacio de información saludable y la cooperación continua es necesaria para garantizar un proceso transparente de lucha contra la desinformación. El Estado por sí solo no es lo suficientemente robusto para operar solo en este campo, por lo que la acción de todos los actores, especialmente la sociedad civil, resulta insoslayable.

5. PROPUESTA DE UNA ESTRATEGIA NACIONAL CONTRA LA DESINFORMACIÓN EN LÍNEA

Una estrategia es, en términos generales, la articulación que una entidad hace para emplear sus recursos disponibles, y así alcanzar sus objetivos y, con ello, materializar la condición que quiere poseer en un horizonte temporal determinado.

Con el propósito de diseñar la presente estrategia, se desarrolló un trabajo de orden deductivo. En primera instancia, se elaboraron algunas definiciones operacionales con el objetivo de precisar el alcance de los diversos conceptos asociados a la noción de desinformación en línea, utilizando distintos referentes. Posteriormente, a fin de establecer la situación actual de este fenómeno en Chile, se desarrolló un análisis colegiado, el cual permitió determinar las distintas variables, sus interrelaciones e impactos.

Posteriormente, se elaboró la presente estrategia, centralizando las diversas iniciativas en torno a tres ejes temáticos: institucionalidad, educación y defensa. Para cada uno de ellos se establecieron iniciativas asociadas a acciones destinadas a lograr un objetivo específico, definiendo responsable y actores involucrados, además de un plazo estimativo.

Los tres ejes son interdependientes, complementarios y coadyuvantes entre sí y todos están estrechamente ligados, de la misma manera como ocurre con las iniciativas.

Considerando que la consecución de cada uno de estos objetivos está directamente vinculada con recursos, especialmente financieros, los plazos establecidos son solo referenciales; asimismo, intentan reflejar una secuencialidad atendiendo a la relación causa-efecto que se produce entre ellos.

A continuación, se presenta un cuadro explicativo de la estrategia a desarrollar, señalando las actividades, acciones, responsables, involucrados, plazos y objetivos para cada eje, donde se mencionan los aspectos a desarrollar:

Estrategia Nacional Contra la Desinformación en Línea 2035 (ESNACDEL-2035)

Eje	Iniciativa	Acción	Responsable	Involucrados	Plazos	Objetivo
Institucionalidad	Elaborar documentos normativos (matriz o complementarios a lo que ya hay)	Promulgación de una Ley Anti-Desinformación, para: • Normar una arquitectura • Regular el comportamiento de y en las redes sociales • Asignar/crear los órganos responsables de responder a cada amenaza identificada, tanto de desinformación como de misinformación. • Regular las operaciones de influencia. • Disponer medidas de defensa y de inteligencia. • Regular el potencial de injerencia extranjera y otras medias para resguardar al país y a su población.	• Congreso	• Otras entidades de gobierno. • Sociedad civil (Colegio de Periodistas, ACHIPEC, etc.)	2023	Generar un marco normativo que regule los aspectos de desinformación operaciones de influencia y otros conceptos relacionados.
	Crear una Agencia Nacional Antidesinformación (**ANAD**) u otro organismo responsable	• Desarrollo de un organismo destinado a coordinar, implementar acciones vinculadas a la prevención en material de desinformación.	• Presidencia • MININT • Congreso Nacional	• SIE • Sociedad civil • Organismos públicos	2024	Contar con un organismo independiente y robusto, en el más alto nivel político responsable de gestionar los esfuerzos nacionales antidesinformación.
	Generar capacidad de gestión y respuesta	• Juegos de guerra y simulacros de emergencia para toma de decisiones y gestión	• ANAD *	• Gobierno • FFAA • EMCO • Infraestructura crítica • SIE • ONEMI • SERVEL • Otros	2024	Preparar los tomadores de decisiones para enfrentar emergencias generadas por el fenómeno.
Institucionalidad	Implementar alianzas internacionales	• Generación de vínculos internacionales de diverso orden, destinados a potenciar iniciativas y medidas.	• MINREL	• ANAD • Sociedad Civil	2024	Incrementar las capacidades de identificación y respuesta antes del fenómeno.
	Establecer relaciones directas con empresas de redes sociales	• Desarrollar relaciones basadas en reglas con empresas de RRSS y media presentes en Chile	• MININT • ANAD	• Empresa privada asociada a RRSS.	2024	Generar comunicación con las empresas para poder limitar campañas dañinas de desinformación.
	Generar capacidades operacionales	• Desarrollar una cultura y una comunidad de verificación de datos.	• Ministerio de Interior • ANAD	• Sociedad civil • MINEDUC	2024	Aumentar la cultura de verificación de datos
		• Desarrollar capacidades de inteligencia de amenazas.	• ANAD • SIE	• FFAA • Carabineros • PDI	2024	Generar capacidades de alerta temprana
		• Desarrollar capacidades tecnológicas y procedimientos.	• MININT • ANAD	• CORFO • Sociedades privadas • Sociedad civil • SIE	2024	Generar tecnología para prevenir y responder al frente del fenómeno
	Garantizar la viabilidad del proyecto a largo plazo	• Sostener la operacionalización de la estrategia. • Garantizar el presupuesto. • Sensibilizar a la opinión pública. • Legitimar la función. • Generar / incrementar las capacidades de comunicación estratégica	• MININT	• Todos los organismos del Estado	2024	Asegurar la permanencia de la institucionalidad desarrollada.

* Una vez conformada esta o el organismo que se implemente para estos fines. Esta nota aplica de aquí en adelante en la presente estrategia.

Eje	Iniciativa	Acción	Responsable	Involucrados	Plazos	Objetivo
Educación	Desarrollar pensamiento crítico mediante educación formal	• Cambio de estrategia curricular en todos los niveles de educación • Implementación de asignaturas destinadas a desarrollo de pensamiento crítico	• MINEDUC • ANAD	• Profesores • Estudiantes • Especialistas en educación	2030	Desarrollar el pensamiento crítico nacional en instancias de educación formal, a objeto de incrementar la capacidad de evaluar la información que se recibe desde medios digitales.
	Capacitar, mediante instancias informales, a los jóvenes y adultos	• Cursos de capacitación gratuitos, financiados por el Estado. • Generación de oferta de cursos de capacitación en el ámbito privado. • Talleres, juegos, mini-videos, quizz	• MINEDUC • ANAD	• Estaciones media • Gobierno Digital • Universidades • Escuelas • Artistas • Influencers • SERVEL	2026	Desarrollar el pensamiento crítico nacional en instancias de educación informal y masiva, a objeto de incrementar la capacidad de evaluar la información que se recibe desde medios digitales.
	Fomentar investigación aplicada en estas temáticas	• Incentivo a productividad académica en estas áreas. • Generación de vínculos internacionales con otras instituciones relevantes.	• MINEDUC • ANAD	• Universidades • MINREL • MINDEF • ANID	2024	Generar conocimiento nuevo sobre el fenómeno su efecto y soluciones.
	Sensibilizar mediante campañas	• Implementación de actividades en MMCS y RRSS	• MININT • ANAD	• MMCS • Gestores de RRSS	2024	Fomentar el conocimiento sobre la desinformación y generar habilidades de identificación de información manipulada.
	Desarrollar instancias de formación de formadores	• Implementación de talleres de desarrollo de capacidades de formación, es estudiantes y monitores.	• MINEDUC • ANAD	• Universidades • Colegios	2024	Desarrollar una modalidad sostenible de educación transversal en la sociedad.
Eje	**Iniciativa**	**Acción**	**Responsable**	**Involucrados**	**Plazos**	**Objetivo**
Defensa, Orden y Seguridad	Actualizar el fenómeno en la doctrina de las FFAA y de Orden	• Revisión y actualización de documentos doctrinarios.	• MININT • MINDEF	• EMCO • FFAA • FFOyS • ANAD	2024	Incorporar el fenómeno en la doctrina institucional, de forma tal de garantizar el manejo seguro de medios y responsabilidad social, en coherencia con lo que se desarrolle en otros sectores de la vida nacional.
		• Incorporación en la malla curricular de los diversos cursos.	• MININT • MINDEF	• EMCO • FFAA • FFOyS • ANAD	2025	Incrementar la educación formal en las diversas instancias formativas de la FF.AA.
		• Implementación de Lecciones Aprendidas.	• CJ Inst. FFAA. • GD Carabineros • DG PDI	• Instituciones • ANAD	2023	Optimizar el desempeño en la prevención y neutralización de las amenazas.
	Entrenar y generar conocimientos en distintas instancias	• Implementación de ejercicios y otras instancias específicas de entrenamiento.	• CJ Inst. FFAA. • GD Carabineros • DG PDI	• Instituciones • ANAD	2024	Entrenar capacidad preventiva y reactiva, como respuesta a acciones de desinformación.
		• Incorporación de la temática en actividades académicas.	• CJ Inst. FFAA. • GD Carabineros • DG PDI	• Instituciones • ANAD	2025	Desarrollar docencia e investigación de frontera, para incrementar la capacidad de respuesta al impacto del fenómeno en un contexto holístico.
	Generar capacidad reactiva y proactiva a través de un organismo especializado	• Organización de entidad de defensa especializada. • Implementación de la doctrina de ciberdefensa activa para la guerra informacional. • Capacitación de analistas. • Desarrollo de capacidades técnicas de análisis.	• MININT • MINDEF	• EMCO • FFAA • FFOyS • ANAD	2025	Generar la capacidad para accionar y reaccionar frente a amenazas informacionales, para identificar y contrarrestar operaciones de influencia digitales

5. CONCLUSIONES

En conclusión, dada la evidencia disponible, se considera fundamental el desarrollo e implementación de una estrategia nacional que dé respuesta a una amenaza que, primero es necesario comprender, para luego poder contrarrestar de manera proactiva.

Los ejes y acciones aquí propuestas abordan las diversas aristas, desde una mirada que permite tanto prevenir, como reaccionar y orientar la vinculación efectiva entre actores. Se debe considerar que este fenómeno irá en aumento, por lo que debe ser abordado en conjunto por todos, de forma multidimensional y multisectorial, para avanzar hacia la defensa de la información efectiva.

En resumen, en el proceso de una estrategia efectiva y eficiente se deben considerar los tres ejes antes señalados, que se resumen en lo siguiente:

Eje 1 Institucionalidad: da cuenta del desarrollo e implementación de un marco normativo y administrativo, que permita ejecutar las acciones regulatorias, preventivas y de respuesta, destinadas a enfrentar la desinformación en línea y sus efectos.

Eje 2 Educación: asumiendo que la lucha contra el fenómeno de la desinformación en línea requiere un cambio cultural profundo, es necesario desarrollar la capacidad tanto colectiva como individual, para operar con ética y protegerse de sus efectos nocivos, a partir de la acción del pensamiento crítico.

Eje 3 Defensa: dado que garantizar la seguridad de los individuos, las instituciones y la sociedad en general es una de las funciones exclusivas del Estado, se debe preparar una capacidad de respuesta a todos los eventos que atenten contra el desarrollo normal de las actividades, tanto desde el exterior como el interior del país.

Como ya se señaló, no existe un modelo perfecto en la lucha contra la desinformación, ya que es un concepto fluido. Pero una cosa es cierta: la inacción frente al fenómeno no es una opción dadas las graves consecuencias sociales que puede implicar.

Los legisladores deberán aprender de los éxitos y críticas de otros países y desarrollar un modelo que pueda funcionar para contrarrestar las operaciones de influencia en el corto, mediano y largo plazo.

*Capítulo 7_*

Interoperabilidad e identidad digital

PARTICIPARON EN LA ELABORACIÓN DE ESTE TEXTO:

- Equipo Coordinador submesa " Interoperabilidad e Identidad Digital": Francisco Mendez y Carla Illanes

- Comité de Trabajo Técnico de la submesa "Interoperabilidad e Identidad Digital" convocado por la Comisión formado por: Berioska Contreras, Marco Zúñiga, César Galindo, Jose Luis Pérez, Álvaro Vásquez, Patricio Ovalle, Ítalo Foppiano y Raimundo Roberts.

Agradecimientos especiales: Ing. Gustavo Giorgetti de Thinknet S.A. Argentina, Ing. Petteri Kivimäki de NIIS, Estonia, Paula Brenes, de Gobernanza Digital, Costa Rica, Diego Philippi, Vor-Tex, Chile, Claudio Reyes, de Gobierno Digital de Chile.

1. INTRODUCCIÓN

Habitamos en el ciberespacio en equivalencia a como habitamos en la ciudad, lo cual nos exige establecer una forma de convivir y relacionarnos de forma segura y confiable.

Para ello y de forma paralela al mundo físico, se deben establecer las condiciones para que la información fluya en infraestructuras seguras y robustas, permitiendo la interacción entre las personas y las instituciones, así como de las instituciones entre si, de manera de permitir los flujos de datos con la mayor confianza posible, sin que se comprometa su integridad, su accesibilidad segura y acreditando trazabilidad.

La confianza digital es la base de una sociedad digital, y esta se construye sobre 2 pilares fundamentales: la identidad digital, y la interoperabilidad. Ambos conceptos desarrollados más adelante y se engarzan con otro ingrediente fundamental: la ciberseguridad.

En el proceso de Transformación Digital del Estado, en que estamos inmersos, la identidad digital y la interoperabilidad deben ser ejes del proceso de transformación que permitan al ciudadano intercatuar en forma segura con los sistemas informáticos del Estado, y lograr así que efectivamente el progreso tecnológico sea un facilitador que mejore la calidad de vida.

El trabajo encomendado a los autores de este capítulo, y de acuerdo a lo que se estableció al convocar a la Mesa de Ciberseguridad, y de acuerdo a la experiencia de los especialistas convocados y considerando algunas publicaciones de Cepal,[26] [27] establecieron dos desafíos a desarrollar relativos a estas materias.

El **primer desafío** es la construcción de una identidad digital robusta, con medios que aseguren no solamente la identidad, sino su autenticación que no deje dudas de quien dice ser para finalmente dar acceso a sistemas informáticos que manejan nuestros datos personales y podamos realizar las interacciones que consideremos necesarias.

Considerando el crecimiento de las transacciones digitales, se requiere avanzar en la identificación y verificación de las personas en el mundo de los servicios digitales. Las tecnologías de identidad digital están evolucionando rápidamente, dando lugar a nuevos modelos de negocio, de servicio y operación, creando una variedad de sistemas que requieren de soporte no sólo tecnológico, sino que también normativo que amplíe su uso tanto privado como público.

[26] "Gobernanza Digital e Interoperabilidad" disponible en: https://repositorio.cepal.org/bitstream/handle/11362/47018/1/S2100258_es.pdf

[27] "La gestión de la identidad y su impacto en la economía global" disponible en: https://publications.iadb.org/es/la-gestion-de-la-identidad-y-su-impacto-en-la-economia-digital

El **segundo desafío**, es la implementación de la interoperabilidad, que sucintamente es el intercambio de informaciones entre múltiples sistemas que manejan data diversa, de forma de que sea compartida electrónicamente en tiempo real desde los lugares donde se almacenan y se procesan. Son los sistemas los que se traspasan entre si la información en términos acotados, y así entre otros beneficios los usuarios pueden obtener informaciones diversas de múltiples fuentes. A mayor abundamiento, el BID (Banco Interamericano de Desarrollo), describía la interoperabilidad como:

"La capacidad de los sistemas TIC de interconectar datos y procesos para compartir información y conocimiento dentro del marco de la protección, la ética y la seguridad, de manera ágil, eficiente y transparente, y con el fín ultimo de tomar decisiones basadas en hechos"

A su vez, la interoperabilidad es un requisito para hacer posible la comunicación digital y el intercambio de información tanto entre las administraciones públicas, como entre éstas y las empresas privadas y organismos no gubernamentales que requieran interacción con el Estado, con la finalidad de lograr un mercado único digital. Si dejamos la interoperabilidad como un tema a resolver entre actores interesados, la complejidad en términos de ciberseguridad se multiplica significativamente.

La interoperabilidad debe ser entendida desde al menos cuatro perspectivas: normativa/legal, de procesos, semántico, y tecnológico en sus respectivas arquitecturas y combinaciones de herramientas disponibles. La experiencia internacional existente reafirma esta distinción, según se explicará más adelante.

Identidad Digital e Interoperabilidad son piezas fundamentales que permiten construir el edificio de la ciberseguridad en cuanto a las relaciones de los usuarios e instituciones en el ciberespacio, y deben estar basados en modelos seguros, robustos y resilientes, de manera que sean una garantía de data segura, y expedita.

En más de 9 reuniones de trabajo tanto presenciales y vituales, algunas plenarias y otras parciales que represenatron más de 40 horas de trabajo, desarrolladas entre el 22 de junio y el 30 de noviembre de 2022, un equipo conformado por profesionales de formaciones diversas entre los que se cuentan abogados, ingenieros, periodistas, empresarios, académicos y militares, lograron el resultado que se refleja en este capítulo. En el se reúnen conceptos y ejemplos obtenidos de las políticas implementadas por otros países. El propósito es estructurar una base teórica, técnica y política, a ser considerados para disponer de una identidad digital robusta e implementar la necesaria interoperabilidad que permita cumplir los objetivos del la ley 21.180 de Modernización Digital del Estado.

2. CONTEXTO

La interoperabilidad esto es, la posibilidad de compartir información de manera segura, ágil y eficiente entre estamentos públicos, así como entre públicos y privados, es un requisito para hacer posible el gobierno electrónico y el intercambio de información entre las administraciones públicas, y entre éstas y las empresas privadas y los organismos no gubernamentales que deban interactuar con el Estado.[28]

La Interoperabilidad dentro del Estado:

→Simplifica la relación del ciudadano, las empresas y las organizaciones con las instituciones del Estado.
→Potencia la cooperación entre las instituciones del Estado con el objeto de resolver las necesidades del ciudadano, las empresas y las organizaciones.
→Incorpora estándares básicos (datos, tecnología, comunicación) en la interacción entre instituciones del Estado.
→Integra instituciones con independencia de su nivel de desarrollo tecnológico.
→Potencia la simplificación administrativa y los procesos en las instituciones y entre ellas.
→Reduce los costos y los esfuerzos, tanto para las instituciones como para el ciudadano, las empresas y las organizaciones.
→Propicia un clima de negocios favorable y competitivo para los países.

Para construir servicios digitales de confianza que fomenten una sociedad segura y mercado digital unificado se requieren transacciones electrónicas con certeza jurídica. Así, haría posible desarrollar el potencial de crecimiento de la economía digital. A modo de ejemplo, se estima que la Unión Europea e Inglaterra alcanzarían un crecimiento asociado por un valor de €1,036.71Bn para 2025.[29]

Tan importante como la certeza jurídica de las transacciones electrónicas es la economía de datos que implica una identidad digital interoperable para el intercambio de documentación y firma digital entre servicios provistos por múltiples gobiernos digitales.

Ahora bien, la expansiva digitalización y conectividad aumenta el riesgo en ciberseguridad, la sociedad es más vulnerable al cibercrimen y ciberamenazas híbridas. Al mismo tiempo, según The Identity Defined Security Alliance, durante lo que va de 2022, el 84% de 504 organizaciones han experimentado brechas de identidad, y el 96% de ellos ha reportado que para minimizar las brechas necesitan fortalecer la seguridad centrada en la identidad.[30]

[28] "Interoperabilidad en gobierno electrónico. Conceptos y regulación extranjera Estonia, Costa Rica y Provincia de Neuquén", Asesoría Técnica Parlamentaria, enero 2023, Biblioteca del Congreso Nacional. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33950/2/Informe_BCN_interoperabilidad_comparado_Est_Neu_CrRc.pdf
[29] https://es.statista.com/Statista GmbH es un portal de estadística que pone al alcance de los usuarios datos relevantes que proceden de estudios de mercado y de opinión
[30] https://www.idsalliance.org/press-release/new-study-reveals-84-of-organizations-experienced-an-identity-related-breach-in-the-last-year/

Considerando lo anterior, y entendiendo que la ciberseguridad constituye un eje habilitante para el desarrollo de un gobierno digital y es la base de la economía digital (involucrando tanto a actores públicos, privados, organizaciones no gubernamentales, ciudadanos y personas) y, que -por su parte- la identidad digital e interoperabilidad contribuyen y habilitan dicho escenario, es que el desarrollo de estos temas será abordado con un enfoque integrador de tipo top down con las siguientes líneas de trabajo como ejes estructurantes:

1. Modelo de Gobernanza: Considerando la complejidad y alcance transversales de los temas de Interoperabilidad e Identidad Digital, se requiere contar con un modelo de Gobernanza que articule a todos los actores que contribuyan al éxito de su implementación en forma horizontal y en los distintos niveles de influencia (Estratégica, Rectora y Ejecutora) de tal forma que se generen los lineamientos, atribuciones, insumos, recursos y capacidades requeridos en el ecosistema en el que intervendrán las habilidades de la interoperación entre actores y la identidad digital para la generación de valor público.

2. Modelo de Institucionalidad: Es necesario contar con legislación actualizada para implementar un modelo de gobernanza. Este deberá desarrollar una institucionalidad definida, que permita establecer atribuciones, estructura organizacional, recursos y modelo de sostenibilidad.

3. Framework de referencia de Interoperabilidad País e Identidad Digital: Especificar las dimensiones de cada tema, estableciendo cobertura e interrelaciones. Se puede mencionar como referencia el marco de interoperabilidad de la Unión Europea (EIF)[31] tanto para Interoperabilidad como para Identidad Digital.

4. Modelo de Generación de valor. La concepción de un Estado moderno en donde sus procesos agregan valor mediante la digitalización en el tratamiento de la información que se requiera desde una institución o empresa a otra y que pueda ser disponibilizada para la mejora en la eficiencia de los procesos, tanto a nivel interno como para favorecer los trámites que la población debe ejecutar.

5. Criterios Tecnológicos a Utilizar: Bilateral o descentralizado, Central, federado, cuatro esquinas u otro. Se puede avanzar en proponer a modo de ejemplo algunas herramientas o plataformas habilitantes en base a experiencia exitosa de otros países.

6. Modelo de Gestión del Cambio y Cultura: Que aborde desde la identificación de las instituciones y grupos objetivos impactados e influyentes, identifique las jerarquías de las resistencias que genera la interoperabilidad y la identidad digital (a nivel técnico y adaptativo), que proponga estructuras de plan de acción para cada dominio de resistencia (Adaptativo, Conocimiento, Información)

[31] https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail

3. MODELO DE GOBERNANZA

La correcta identificación de los actores involucrados, sus grados de influencia y jerarquías en la toma de decisiones, es un aspecto clave para el éxito de la ciberseguridad y, dentro de ésta, la interoperabilidad e identidad digital.

Para desarrollar esto, es necesario contar con una definición de referencia de qué se entenderá por Gobernanza:

La gestión de relaciones entre diversos actores involucrados en el proceso de decidir, ejecutar y evaluar asuntos de valor público, proceso que puede ser caracterizado por la competencia y cooperación donde coexisten como reglas posibles; y que incluye instituciones tanto formales como informales. La forma e interacción entre los diversos actores refleja la calidad del sistema y afecta a cada uno de sus componentes; así como al sistema como totalidad.

Los actores involucrados en el proceso de decidir es un factor clave para las distintas instancias de la Gobernanza que se detallan más adelante. En esta identificación se debe tener en cuenta el nivel de Impacto que tendrá en su quehacer diario la ciberseguridad (impacto en la generación de beneficios como en los cambios en actividades habituales) como también la identificación de la Influencia de los actores involucrados. Ambos conceptos son presentados en el punto de Gestión del Cambio.

Dada la distinta naturaleza de los actores involucrados en el proceso de logro en la implementación de la Ciberseguridad, Cepal propone las siguientes clasificaciones o jerarquías de Gobernanza asociadas a Gobierno Digital que se pueden extrapolar y/o identificar como requerimientos para Ciberseguridad, a saber:

Gobernanza Estrategica	Establece Prioridades, Políticas, Estrategias, Involucrados, Atribuciones
Gobernanza Rectora	Establece Leyes, Normas, Reglas, Metodologías Plazos, Roles, Audita cumplimiento
Gobernanza Ejecutora	Define, diseña, implementa, asiste, acompaña, resuelve

En donde:

→**Gobernanza Estratégica:** contribuye a la articulación y coordinación de los distintos sectores (o instituciones relacionadas), en la búsqueda de identificar componentes de valor compartido que sólo es factible alcanzar en un accionar conjunto y coordinado, para lo cual se requiere contar con las atribuciones vinculantes para convocar, priorizar, asignar recursos y construir planes compartidos y comprometer resultados.

→**Gobernanza Rectora:** contribuye en la identificación de leyes, normas técnicas, reglas, roles, metodologías y auditorías de cumplimiento (evaluación de impacto de las iniciativas), así como también la definición, diseño e instrucciones de implementación de los pilares de soluciones transversales del Gobierno Digital como lo son la Interoperabilidad País, Identidad Digital, Firma Digital, Casilla Digital, Carpeta Digital, Ventanilla única, Ciberseguridad y cualquier otra solución transversal a las instituciones como pueden ser: gestión de personas, contabilidad, presupuesto, gestión documental, Domicilio Digital Único u otra.

→**Gobernanza Ejecutora:** contribuye a la implementación de las soluciones de Gobierno Digital en sus componentes de Procesos, Personas y Tecnología de la Información habilitante. Articulando plataformas, herramientas tecnológicas, profesionales especializados, mediante equipos propios, contratación de servicios de soluciones de aplicaciones y/o desarrollo de terceros.

Cada ámbito de gobernanza contribuye, desde su accionar, a que fluyan desde lo horizontal hacia lo vertical (articulación de actores, recursos, iniciativas; en lo estratégico, Rector y ejecutor) y entre cada ámbito de gobernanza, en ciclos coordinados de acciones y actores con una finalidad y propósito compartido que contribuya a que el Gobierno digital sea factible y genere el valor público esperado y comprometido.

Esto se materializa con una estructura de gobierno que contempla al menos:

→**Materialización de la Gobernanza Estratégica:** Consejo de Ministros en donde se instale en forma permanente el eje de Ciberseguridad y/o una Comisión de alto nivel de Gobierno Digital que defina, priorice y valide políticas e iniciativas de interés Estado y, actué como directorio procurando que algunos de los miembros sean de carácter permanente para mitigar los efectos de los cambios en los períodos presidenciales.[32]

[32] Actualmente, existen tres instancias de alto nivel que ven temas relacionados directa o indirectamente con estos aspectos:
1.Consejo Asesor Permanente para la Modernización del Estado y el Comité de Modernización del Estado: ambos establecidos en el Decreto N°5, de 2021 (que modifica el Decreto N° 12, de 2018, del Ministerio de Hacienda (https://www.bcn.cl/leychile/navegar?idNorma=1163311&idParte=10256530) que tiene un objeto más amplio, pues pretende "asesorar al Presidente de la República en el análisis y evaluación de las políticas, planes y programas que compongan la agenda de modernización del Estado; formular recomendaciones sobre tales materias; someter a su consideración, propuestas de reforma estructural o institucional para ser llevadas a cabo como iniciativas de ley o dentro de las competencias que en materia de organización interna le confiere el ordenamiento jurídico; y dar respuesta a las consultas que dicha autoridad le formule" (art.2).
2.Comité Interministerial de Ciberseguridad: el Decreto N° 533, de 2015 (modificado por el Decreto N°579, de 2020 creó el Comité Interministerial de Ciberseguridad, "...cuya misión es proponer una política nacional de ciberseguridad, sugerir alternativas de seguimiento a su avance e implementación, y asesorar en la coordinación de acciones, planes y programas en materia de ciberseguridad de los distintos actores públicos y privados en la materia."
Resulta claro que este último tiene como finalidad tratar temas específicos de ciberseguridad, pero no abarca materias de identidad digital o interoperabilidad.

→**Materialización de la Gobernanza Rectora:** un ente (Agencia, Ministerio u otro) que canalice y de gobierno a las iniciativas de interés del Estado a nivel transversal. Para ésto se requiere de una institucionalidad que tenga las atribuciones transversales vinculantes para definir modelos, marcos normativo legales, marcos técnicos y apoyo respecto de habilitantes tecnológicos transversales como lo son: Identidad Digital, Interoperabilidad y ciberseguridad.

→**Materialización de la Gobernanza Ejecutora:** un ente que lleve a cabo en términos de implementación, soporte, mantenimiento y continuidad operacional, las soluciones transversales que se definan y, los habilitantes tecnológicos.

4. MARCO REGULATORIO DE LA INTEROPERABILIDAD E IDENTIDAD DIGITAL EN CHILE HOY

4. 1. Interoperabilidad

En la actualidad, nuestro país no cuenta con una norma general expresa sobre interoperabilidad, aún cuando, al interior de la Administración, las transferencias de información se hanasado en el principio de cooperación que rige a los órganos públicos, conforme DFL 1/DFL 1-19653,[33] de 2001, que fija texto refundido, coordinado y sistematizado de la ley N° 18.575, orgánica constitucional de la bases generales de la Administración del Estado,

Por su parte, la dictación de la ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma trajo un enorme cambio a esta habilitación legal, pues mediante una de sus normas técnicas se introdujo por primera vez el concepto de interoperabilidad, determinando obligaciones y entidad encargada de la dictación de estándares.

Posteriormente, la ley N° 19.880, que establece Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la Administración del Estado incorporó ciertos principios rectores que sirvieron para apalancar la transferencia de datos, pero siempre bajo una óptica de cooperación. Solo la dictación de la ley N° 21.180 significó un cambio trascendental, según se expondrá.

Ley N° 19.880 que establece Bases de los Procedimientos Administrativos que rigen los actos de los órganos de la Administración del Estado

[33] "Artículo 5º.- Las autoridades y funcionarios deberán velar por la eficiente e idónea administración de los medios públicos y por el debido cumplimiento de la función pública.
Los órganos de la Administración del Estado deberán cumplir sus cometidos coordinadamente y propender a la unidad de acción, evitando la duplicación o interferencia de funciones."

Incorpora, en su artículo 14, a nivel de principio, el de inexcusabilidad, al establecer en su inciso 2°: *"Requerido un órgano de la Administración para intervenir en un asunto que no sea de su competencia, enviará de inmediato los antecedentes a la autoridad que deba conocer según el ordenamiento jurídico, informando de ello al interesado."* De esta forma, establece la obligación de interoperar antecedentes (en sentido amplio).

Además, incorpora como un derecho de las personas en su relación con la Administración, el eximirse de presentar documentos que ya obren en poder de esta (art. 17 letra d)[34]

Decreto N° 14, de 2014, del Ministerio de Economía, Fomento y Turismo, Modifica Decreto N° 181, de 2002, que aprueba Reglamento de la Ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y la Certificación de dicha firma, y deroga los decretos que indica

La citada norma técnica de la ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma, fue el primer cuerpo normativo en establecer la facultad del Ministerio Secretaría General de la Presidencia de proponer las normas técnicas que deberán seguir los órganos de la Administración del Estado para, entre otros aspectos, **garantizar la interoperabilidad en el uso de documentos electrónicos.** De esta forma, el enfoque de esta normativa se encontraba en la interoperabilidad de documentos electrónicos y entre órganos de la Administración del Estado (art. 47).

Ley N° 21.180, de Transformación Digital del Estado

La dictación de esta ley cambió el paradigma en materia de interoperabilidad, pues se determinó su establecimiento como un principio de los medios electrónicos (art. 16 bis nuevo de la ley N° 19.880)[35] y un estándar de las plataformas electrónicas de gestión de expedientes (art. 19 -modificado- de la ley N° 19.880). De esta forma, la interoperabilidad por primera vez es un principio - obligatorio- en la interacción entre órganos de la Administración del Estado, y abarca más allá de los documentos electrónicos, pues la ley habla de los medios electrónicos.[36]

Así, el legislador potencia la transferencia de información al interior de la Administración, idea de lo cual también da cuenta el art. 24 bis de la ley N° 19.880, al prescribir: *"En virtud de los principios de interoperabilidad y cooperación, en todo procedimiento administrativo, los órganos de la Administración del estado*

[34] Art. 17 letra d): "Eximirse de presentar documentos que no correspondan al procedimiento o que emanen y se encuentren en poder de cualquier órgano de la Administración del Estado. En este último caso, dichos documentos deberán ser remitidos por el órgano que los tuviere en su poder a aquel que estuviere tramitando el procedimiento administrativo"

[35] El art. 16 bis lo define como:"El principio de interoperabilidad consiste en que los medios electrónicos deben ser capaces de interactuar y operar entre sí al interior de la Administración del Estado, a través de estándares abiertos que permitan una segura y expedita interconexión entre los mismos."

[36] Si bien la ley no define medio electrónico, si se hacen referencias en la Historia de la Ley, donde se definieron como: "Son las formas a través de las cuales los documentos o los insumos electrónicos se entregan. Puede tratarse de un video, de un documento electrónico, de un audio o de datos de una base de datos. Esta información puede ser almacenada en un expediente electrónico y ser guardada e integrada en un procedimiento administrativo." Disponible en Primer Informe de la Comisión de Gobierno Interior, Nacionalidad, Ciudadanía y Regionalización, de 26 de junio de 2019.

que tengan en su poder documentos o información respecto de materias de su competencia, que sean necesarios para su conocimiento o resolución, deberán remitirlos por medios electrónicos, a aquél órgano ante el cual se estuviere tramitando el respectivo procedimiento, que así lo solicite."

4. 2. Identidad Digital

Nuestro país tampoco cuenta con una norma específica que regule la identidad digital en su conjunto, sino que se trata de referencias normativas (una de ellas ya derogada y otra en trámite) a la autenticación y a la firma electrónica, según se describirá.

Ley N° 19.477, de 1996, que aprueba Ley Orgánica del Servicio de Registro Civil e Identificación

En su artículo 4° reconoce como una función del Servicio el establecer y registrar la identidad civil de las personas y otorgar los documentos oficiales que la acrediten.

En ese sentido, el artículo 33 N° 5 de la norma citada, contempla como obligación de los Oficiales Civiles "...supervisar el correcto otorgamiento de las cédulas de identidad, pasaportes y demás documentos de identificación que se tramiten en su Oficina".

Ley N° 19.799, de 2002, sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma

La letra e) del artículo 12 esta ley, dispone que es obligación del prestador de servicios de certificación de firma electrónica en el otorgamiento de certificados de firma electrónica avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del Registro Civil, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica.

Este artículo sirve de base para el Decreto N° 24, de 2019, de MINECON, que se tratará más adelante.

Esta ley, según lo señala su nombre es la única que regula en profundidad en Chile todos los temas derivados de la firma electrónica

[Derogado] Decreto N° 77, de 2004, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la Administración del Estado y entre estos y los ciudadanos; derogado por el Decreto N° 14, de 2014, del Ministerio de Economía, Fomento y Turismo

Ámbito de aplicación:

→Las comunicaciones realizadas por medios electrónicos.
→Que tuvieran lugar tanto entre órganos de la Administración del Estado, como entre éstos y las personas.
→En toda esfera no regulada por otras normas legales, reglamentarias o administrativas específicas.

Menciones a la autenticación:

→ La primera mención se realizaba en el artículo 4: en la medida que un servicio público interactuare a través de un sitio web con personas (naturales y jurídicas) y que existiera una página de inicio asociada a una dirección de Internet (URL) específica, los órganos de la Administración debían declarar los formatos y medios compatibles con sus sistemas para efectos de enviarse correos electrónicos y/o autenticarse y acceder al sitio.

→ Por su parte, el artículo 11 establecía que, con la finalidad de proteger la confidencialidad de la información en las comunicaciones, se podía utilizar un mecanismo de autenticación o de control de acceso a las direcciones electrónicas que contenían las respuestas que otorgaba la Administración del Estado a las personas.

Decreto Supremo N° 83, de 2005, del Ministerio Secretaría General de la Presidencia que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

Define "autenticación" como el proceso de confirmación de la identidad del usuario que generó un documento electrónico y/o que utiliza un sistema informático (literal a] del artículo 5)

Por su parte, la letra k) del citado artículo conceptualiza al "Identificador formal de autenticación" como un mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos[37]. Más tarde consigna que el uso de este mecanismo es básico para el uso de firma electrónica.

Así también, indica que la seguridad de un documento electrónico se alcanza garantizando -entre otros- su factibilidad de autenticación, entendida como uno de los atributos esenciales del documento.

Decreto N° 14, de 2014, del Ministerio de Economía, Fomento y Turismo, Modifica Decreto N° 181, de 2002, que aprueba Reglamento de la Ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y la Certificación de dicha firma, y deroga los decretos que indica.

[37] Art. 17 letra d): "Eximirse de presentar documentos que no correspondan al procedimiento o que emanen y se encuentren en poder de cualquier órgano de la Administración del Estado. En este último caso, dichos documentos deberán ser remitidos por el órgano que los tuviere en su poder a aquel que estuviere tramitando el procedimiento administrativo"

En su articulado transitorio, en su numeral 1.2 sobre Normas Técnicas para las Comunicaciones Electrónicas, hace una referencia vaga a las formas de acceso a las comunicaciones electrónicas, precisando en su literal b) que corresponde a los órganos de la Administración del Estado tomar las medidas de seguridad tendientes a evitar la interceptación, obtención, alteración y otras formas de acceso no autorizado a sus comunicaciones electrónicas. En todo esto señala que se deberá estar a lo dispuesto en las normas técnicas establecidas en el Decreto Supremo N° 83, de 2005, del Ministerio Secretaría General de la Presidencia.

Decreto N° 24, de 2019, del Ministerio de Economía, Fomento y Turismo, que aprueba Norma Técnica para la prestación del servicio de certificación de firma electrónica avanzada.

En sus considerandos define ClaveÚnica como un mecanismo de identificación digital que permite a los usuarios demostrar su identidad en plataformas digitales, ya que el Servicio de Registro Civil e Identificación verifica que la identidad digital corresponde a determinada persona, validándola contra su base de datos.

Además, establece que la ClaveÚnica es un mecanismo digital de comprobación de identidad del solicitante de un certificado de firma electrónica avanzada, en los términos exigidos por el artículo 12 letra e) de la ley de firma.

[En trámite] Norma Técnica de Autenticación, derivada de la Ley de Transformación Digital del Estado.

Establece a ClaveÚnica como mecanismo oficial de autenticación para el acceso de los interesados a las plataformas electrónicas de la Administración.

El proceso de enrolamiento a ClaveÚnica y el servicio de atención a personas naturales a este respecto, depende del Servicio de Registro Civil e Identificación.

Consigna que se trata de un Mecanismo Oficial de Autenticación que administra el Ministerio Secretaría General de la Presidencia a través de su División de Gobierno Digital, que valida los datos de identificación de personas naturales basado en el estándar OpenID Connect cuyo factor de autenticación es una contraseña creada y administrada por la persona, vinculada a su rol único nacional (RUN). Permite la habilitación de ClaveÚnica a los órganos de la Administración del Estado, la infraestructura de la plataforma, el monitoreo de su correcto funcionamiento y la validación de los datos de identificación.

Por su parte, determina que la Clave Tributaria será el mecanismo de autenticación para personas jurídicas y entes y agrupaciones sin personalidad jurídica.

Con todo, establece la posibilidad de creación de nuevos mecanismos de autenticación por parte de los órganos de la Administración del Estado, siempre y cuando estos cumplan los requisitos técnicos establecidos en la misma norma y sean validados por la División de Gobierno Digital.

5. ENTORNOS DE TRABAJO DE INTEROPERABILIDAD

La interoperabilidad es la capacidad de que las organizaciones interactúen con vistas a alcanzar objetivos comunes que sean mutuamente beneficiosos y que hayan sido acordados previa y conjuntamente, recurriendo a la puesta en común de información y conocimientos entre las organizaciones, a través de los procesos institucionales a los que apoyan, mediante el intercambio de servicios, datos y/o documentos entre sus sistemas de TIC respectivos (Comisión Europea, 2010). Es un enfoque de agregación de valor en la prestación de servicios de una forma interoperable.

La interoperabilidad gubernamental es un requisito para hacer posible la comunicación digital y el intercambio de información automatizada entre las administraciones públicas, entre éstas y las empresas privadas y organismos no gubernamentales que requieran interacción con el Estado, con la finalidad de lograr un mercado único digital.

Durante los últimos 20 años en Chile, la conversación respecto a la interoperabilidad ha estado principalmente relacionada con la interoperabilidad entre órganos del Estado. Algunas iniciativas de Interoperabilidad entre agentes del mundo privado y el sector público, o entre entidades del sector privado, han dado curso a algunas iniciativas específicas, como los modelos de EDI (Electronic Data Interchange) para el sector Exportador/importador en la década del 90 y algunas iniciativas de intercambio de información al interior de la industria financiera.

Pero sin lugar a duda, Chile carece de una mirada sistemática que, en las diversas dimensiones indicadas, permita establecer iniciativas nacionales que generen oportunidades de colaboración multisectorial. Y ello a pesar que hay procesos que interoperan, aunque de forma limitada entre instituciones.[38] [39]

5.1 Dimensiones de la interoperabilidad

Siguiendo el marco europeo de interoperabilidad[40] y la publicación de gobernanza digital e interoperabilidad gubernamental de la CEPAL,[41] se determinan cuatro niveles o dimensiones de interoperabilidad:

[38] https://www.latercera.com/opinion/noticia/interoperabilidad-un-nuevo-escenario-para-la-modernizacion-del-estado/DMKBEH4IWJE7BPIM5XFTMZU6JM/

[39] https://digital.gob.cl/plataformas-transversales/

[40] Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52017DC0134&from=LT#:~:text=El%20Marco%20Europeo%20de%20Interoperabilidad%20es%20un%20enfoque%20concertado%20con,principios%2C%20modelos%20y%20recomendaciones%20comunes.

[41] A. Naser (coord.), "Gobernanza digital e interoperabilidad gubernamental: una guía para su implementación", Documentos de Proyectos (LC/TS.2021/80), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2021.

→**Interoperabilidad legal o jurídica:** Consiste en garantizar que las organizaciones que operan bajo diferentes marcos jurídicos, políticas y estrategias pueden trabajar juntas. Deben existir acuerdos claros sobre cómo abordar las diferencias en la legislación, incluida la opción de adoptar una nueva legislación.

El primer paso es realizar «controles de interoperabilidad» mediante el examen de la legislación existente para detectar los obstáculos a la interoperabilidad. Identificar requisitos contradictorios para procesos institucionales iguales o similares, seguridad y necesidades de protección de datos obsoletas, etc. Debe valorarse la coherencia de la legislación, con vistas a garantizar la interoperabilidad. La legislación propuesta debe someterse a un «control digital» para:

*Garantizar que no sólo se adecúa al mundo físico sino también al digital;

*Identificar los obstáculos al intercambio digital; y

*Determinar y evaluar el impacto de las TIC en las partes interesadas.

Esto facilitará y aumentará el potencial de reutilización de las soluciones de TIC existentes, reduciendo así los costos y el plazo de implantación.

→**Interoperabilidad organizativa:** : significa que los servicios estén disponibles, sean fácilmente identificables, sean accesibles y estén centrados en el usuario. Tiene dos componentes:

i. Alineamiento de los procesos institucionales: Todas las instituciones públicas que contribuyan a la prestación de servicios públicos deben entender globalmente (de extremo a extremo) el proceso institucional y su función dentro del mismo.

ii. Relaciones institucionales: Estructurar claramente la relación entre los proveedores de los servicios y sus consumidores. Obliga a encontrar instrumentos que permitan formalizar la asistencia mutua, la actuación conjunta y los procesos institucionales interconectados, por ejemplo, los MoU (Memorandum of Understanding o acuerdos de colaboración) y SLA (Service Level Agreements o acuerdos de nivel de servicio), entre las administraciones públicas participantes.

→**Interoperabilidad semántica:** Garantizar que el formato y el significado exacto de la información intercambiada se comprendan y conserven en todos los intercambios entre las partes, es decir, «que lo que se transmite sea lo que se entiende». Aspectos semánticos y sintácticos:

*El aspecto semántico se refiere al significado de los elementos de datos y la relación entre ellos. Incluye la creación de vocabularios y esquemas para describir los intercambios de datos y garantiza que todas las partes que se comunican entienden de la misma manera los elementos de datos;

*El aspecto sintáctico se refiere a la descripción del formato exacto de la información que se va a intercambiar en términos de gramática y formato.

Un punto de partida para la mejora de la interoperabilidad semántica consiste en percibir los datos y la información como un valioso bien público. Los acuerdos sobre los datos de referencia en forma de taxonomías, vocabularios controlados, tesauros, listas de códigos y estructuras y modelos de datos reutilizables constituyen requisitos clave para alcanzar la interoperabilidad semántica.

→**Interoperabilidad técnica:** Abarca las aplicaciones e infraestructuras que conectan sistemas y servicios. Incluye elementos tales como especificaciones de interfaz, servicios de interconexión, servicios de integración de datos, presentación e intercambio de datos y protocolos de comunicación seguros.

El BID (2019), complementa este dominio con los siguientes subdimensiones:

***Arquitectura Institucional:** implementar la tecnología de software de una manera estructurada y organizada, con un enfoque en la gobernanza y con el fin claro de cumplir con los objetivos establecidos y asegurar los enlaces de desarrollo de software entre múltiples áreas de una institución, o entre instituciones, tanto dentro como fuera de las TI.

***Normas o estándares técnicos:** conjunto de requisitos, especificaciones, pautas o características que se pueden usar de manera consistente para garantizar que la tecnología de la información a implementar y los procesos se ajusten a su propósito. Los estándares proporcionan un lenguaje común y un conjunto de expectativas que permiten la interoperabilidad entre sistemas y/o dispositivos. De estos hacen parte los estándares para el intercambio, transmisión, mensajería, seguridad y privacidad. Se incluyen aspectos de la metodología de desarrollo de la arquitectura institucional, así como metodologías ágiles para la gestión de proyectos y las denominadas DevOps como una forma innovadora de desarrollo de programas informáticos + operaciones de tecnología de la información.

***Operación y mantenimiento:** desarrollar procesos óptimos de gestión, operación, monitoreo y mantenimiento para asegurar su disponibilidad, continuidad y seguridad bajo los acuerdos de niveles de servicio establecidos entre las partes.

***Equipos informáticos y redes de acceso:** elementos de infraestructura necesarios para el despliegue y ejecución de los programas, plataformas, servidores de aplicaciones y contenedores, así como los entornos de ejecución, las aplicaciones empaquetadas, las máquinas virtuales, etc., que se encuentran en el hardware y son necesarios.

***Redes de comunicación:** Comprender cómo se configuran y establecen las redes para alinear los niveles de servicios y los planes de continuidad, y adecuarlas a las estrategias ya conceptualizadas en otros dominios.

***Gestión de datos:** incluye, aunque no exclusivamente, su recopilación, visualización, almacenamiento, intercambio, agregación y análisis. Concepto central de la gestión de datos es la responsabilidad, corresponde a un administrador debidamente nombrado, quien se ocupa de garantizar el uso adecuado de la información, y de prevenir y evitar usos incorrectos. Los datos son un activo de las instituciones, y en ese sentido se deben tratar y proteger como cualquier otro activo.

Las principales funciones de la gestión de datos son las siguientes:

→Gobernanza de datos: planificación, supervisión y control en la gestión y uso de datos.

→Arquitectura de datos: diseño de los modelos, políticas y reglas para gestionarlos.

→Modelado y diseño de datos: diseño, implementación y soporte de la base de datos.

→Almacenamiento de datos: función que determina cómo, cuánto y qué se almacena.

→Seguridad de los datos: todo lo relativo a la privacidad, confidencialidad y acceso apropiado.

→Integración e interoperabilidad de datos: función relativa a su integración y transferencia.

→Documentos y contenidos: comprende las reglas aplicables a los datos por fuera de las bases de datos.

→Referencia y datos maestros: ofrece una visión de 360° sobre la información, sus propiedades y consentimiento.

→Almacenamiento de datos e inteligencia del negocio (BI): todo lo referente a datos históricos y analíticos.

→Metadatos: conjunto de datos que describen el contenido informativo de un recurso, de archivos o de información de estos. Es decir, es información que describe otros datos.

→Calidad de los datos: refiere a la definición, control y mejora de su calidad.

5. 2 Dominios de la interoperabilidad

***Gobernanza de la interoperabilidad:** Se refiere a las decisiones sobre los marcos de interoperabilidad, los acuerdos institucionales, las estructuras organizativas, las funciones y responsabilidades, las políticas, los acuerdos y demás aspectos cuyo objetivo es garantizar y supervisar la interoperabilidad.

***Gobernanza de los servicios públicos integrados:** Los servicios deben gobernarse con el fin de garantizar: la integración, la ejecución ininterrumpida, la reutilización de servicios y datos y el desarrollo de nuevos servicios.

***Dominio Personas:** el BID (2019) incluye en este dominio el conjunto de principios, pautas y normas que una institución adopta para ayudar a administrar el personal. El mantenimiento de un sistema interoperable requiere de una institución altamente entrenada. En la etapa de operación y mantenimiento, la institución deberá contar con un equipo técnico que lleve adelante estas tareas y con un equipo de proyectos que desarrolle y amplíe las capacidades. Se estructura en dos subdominios:

***Habilidades:** dotación suficiente y sostenible de personal con la combinación adecuada de habilidades para respaldar a la institución en los ámbitos del sector social. Existe un plan estratégico de recursos humanos para mejorar sus competencias, de modo que puedan ejecutar las mejores prácticas internacionales.

***Desarrollo de capacidades:** actividades de entrenamiento y formación dirigidas a impartir conocimientos, formar competencias y capacidades específicas en el personal, y a moldear actitudes, todo ello con el propósito de obtener resultados de aprendizaje claros y así mejorar los resultados de la interoperabilidad.

6. ENTORNOS DE TRABAJO DE IDENTIDAD DIGITAL

Una identidad digital es una representación única de un sujeto dispuesto a realizar una transacción electrónica (NIST, 2017). A su vez, la identificación permite relacionar un conjunto de características de una entidad generalizada para precisar una identidad única en el contexto de un servicio digital de valor. La legitimidad de una identidad digital se comprueba a través de autenticadores que otorgan, o no, el acceso a datos protegidos. Una vez que se ha comprobado la validez de una identidad se establecen relaciones de confianza entre las entidades que interoperan entre sí, es decir, entre ciudadanos digitales, organizaciones privadas y autoridades públicas (EU EIF, 2017). Una identidad digital confiable se funda, además, en los principios de seguridad de autenticidad y no repudio, que buscan garantizar una entidad genuina, y evitar el desconocimiento o rechazo arbitrario de una acción, correspondientemente.[42]

[42] Identidad digital: conceptos y legislación", Asesoría Técnica Parlamentaria, octubre de 2022, Biblioteca del Congreso Nacional. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33658/2/Identidad_Digital_BCN_2022.pdf

Existen múltiples definiciones de Identidad Digital, dependiendo el contexto, en términos generales entenderemos la Identidad Digital como el conjunto de atributos de información que permiten distinguir en forma individual y única a una persona natural, una entidad jurídica o un objeto de información, que permite su presencia y sus interacciones en el mundo digital.

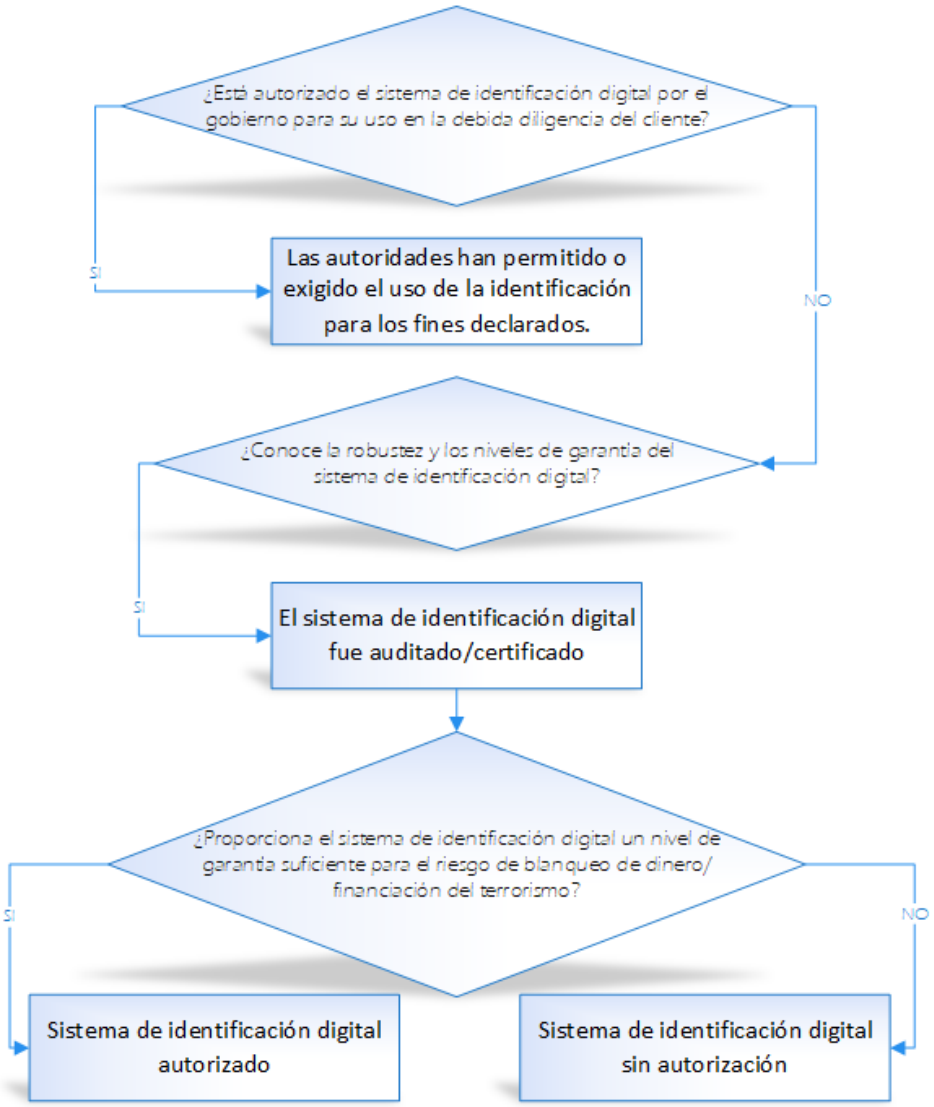
En el caso de las personas, la identidad digital permite entre otros servicios, el aplicar mecanismos criptográficos al contenido de un mensaje o documento con el objetivo de demostrar al receptor del mensaje que el emisor del mensaje es real (autenticación), que éste no puede negar que envió el mensaje (no repudio) y que el mensaje no ha sido alterado desde su emisión (integridad).

En consecuencia, la Identidad Digital es un elemento fundamental para la implementación, entre muchos otros servicios, de la firma digital, ya sea en sus expresiones de firma electrónica avanzada o firma electrónica cualificada o aquella que se ha denominado "simple".

6. 1 Acerca de los Sistemas de Identidad Digital

Un sistema de identidad provee los requerimientos que permiten seleccionar algún nivel de garantía en términos de identificación, autenticación y autorización. Los sistemas de identidad deben comprobar la legitimidad de una identidad combinando autenticadores, credenciales, y aseveraciones, entre otros. La definición de niveles de garantía corresponde a la regulación. De hecho, el reconocimiento o clasificación de un sistema de identidad digital debe ser regulado. La siguiente figura ilustra las fases generalizadas por las que debe transitar un sistema de identidad digital para su uso a nivel gubernamental (CEPAL, 2022).

Los niveles de garantía o seguridad determinan los procesos de comprobación de identidad, autenticación o federación. Además, la firma digital puede integrarse a los procesos de verificación de identidad, en distintas formas, por ejemplo: firma electrónica simple, firma electrónica avanzada y firma electrónica cualificada.



Firma Electrónica

A veces también llamada e-firma, concepto jurídico, equivalente electrónico al de la firma manuscrita, donde una persona acepta y da por validado el contenido de un mensaje electrónico a través de cualquier medio electrónico que sea legítimo y permitido. Ejemplos:

***** Usando una firma biométrica.

***** Firmando con un lápiz electrónico

***** Al usar una tarjeta de crédito o débito en un comercio.

***** Marcando una casilla en una computadora, a máquina, o aplicada con el ratón o incluso con el dedo del usuario en una pantalla táctil.

*****Usando una firma digital.

* Usando un sistema que obligue a establecer usuario y contraseña.
* Usando una tarjeta de coordenadas.

La firma electrónica a su vez puede tener diferentes técnicas para firmar un documento, así tenemos las siguientes:

***Código secreto o de ingreso:** es la necesidad de una combinación determinada de números o letras, que son sólo conocidas por el dueño del documento, o lo que todos usamos por ejemplo en los cajeros automáticos, el conocido PIN (Personal Identification Number);

***Métodos basados en la Biometría:** se permite el acceso al documento mediante mecanismos de identificación física o biológica del usuario o dueño del documento; la forma de identificación en este caso consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos, Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz).

***Perfeccionamiento del cifrado de mensajes**, que se conoce como criptografía, que consiste en un sistema de codificación de un texto con llaves de carácter confidencial y procesos matemáticos complejos, de manera que para el tercero resulta incomprensible el documento si desconoce la clave decodificadora, que permite visualizar el documento en su forma original; de ahí es que surgen dos tipos de criptografía:

→**De llave secreta o simétrica:** las partes en los dos procesos de cifrado y descifrado comparten una llave común previamente acordada; debe ser conocida solamente por ambas partes, para evitar que un tercero ajeno a la operación pueda descifrar el mensaje transmitido y de esa forma hacer caer toda la seguridad del sistema.

→**De llave asimétrica o llave pública:** Este sistema posee dos llaves: llave privada y llave pública. Una de ellas sólo es conocida por el autor del documento y la otra puede ser conocida por cualquier persona; si bien esas dos llaves se encuentran relacionadas matemáticamente mediante un algoritmo, no es posible por medio de la llave pública, conocer la llave privada, por lo menos en los estándares tecnológicos actuales.

Una firma electrónica crea un historial de auditoría que incluye la verificación de quién envía el documento firmado y un sello con la fecha y hora.

La firma electrónica ofrece seguridad y respaldo legal. En el caso de las firmas electrónicas avanzadas y cualificadas, además de identificar al firmante de forma única, garantizan la integridad de la información contenida en el mensaje o documento.

La validez de una firma se ampara en la imposibilidad de falsificar cualquier tipo de firma, siempre y cuando se mantenga en secreto la clave del firmante. En el caso de las firmas escritas el secreto está constituido por características de tipo grafológico inherentes al signatario y por ello difíciles de falsificar. Por su parte, en el caso de las firmas digitales, el secreto del firmante es el conocimiento exclusivo de una clave (secreta) utilizada para generar la firma. Para garantizar la seguridad de las firmas digitales es necesario a su vez que estas sean:

***Únicas:** Las firmas deben poder ser generadas solamente por el firmante y por lo tanto infalsificable. Por tanto, la firma debe depender del firmante.

***Infalsificables:** Para falsificar una firma digital el atacante tiene que resolver problemas matemáticos de una complejidad muy elevada, es decir, las firmas han de ser computacionalmente seguras. Por tanto, la firma debe depender del mensaje en sí.

***Verificables:** Las firmas deben ser fácilmente verificables por los receptores de estas y, si ello es necesario, también por los jueces o autoridades competentes.

***Innegables:** El firmante no debe ser capaz de negar su propia firma.

***Viables:** Las firmas han de ser fáciles de generar por parte del firmante.

Firma Electrónica Avanzada

Firma electrónica que cumple los siguientes requisitos:

*Estar vinculada al firmante de manera única;

*Permitir la identificación del firmante;

*Haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo,

*Estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Firma Electrónica Cualificada

Firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

¿Cuál es la principal diferencia entre la firma electrónica avanzada y la cualificada?

Considerando las definiciones del reglamento eIDAS, la principal diferencia entre la firma electrónica avanzada y la cualificada son dos:

*La firma electrónica cualificada se debe crear con un dispositivo cualificado de creación de firmas electrónicas.

*La firma electrónica cualificada debe de estar basada en un certificado cualificado de firma electrónica.

¿Qué es un dispositivo cualificado de creación de firmas electrónicas?

Los dispositivos cualificados de creación de firmas electrónicas deben cumplir con los requisitos de los dispositivos cualificados de creación de firma electrónica establecidos en el Anexo II del Reglamento 910/2014.[43]

Requisitos de los dispositivos cualificados de creación de firma electrónica

1. Los dispositivos cualificados de creación de firma electrónica garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:

a) Esté garantizada razonablemente la confidencialidad de los datos de creación de firma electrónica;

b) Los datos de creación de firma electrónica utilizados para la creación de firma electrónica sólo puedan aparecer una vez en la práctica;

c) Exista la seguridad razonable de que los datos de creación de firma electrónica utilizados para la creación de firma electrónica no pueden ser hallados por deducción y de que la firma está protegida con seguridad contra la falsificación mediante la tecnología disponible en el momento;

d) Los datos de creación de la firma electrónica utilizados para la creación de firma electrónica puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros.

2. Los dispositivos cualificados de creación de firmas electrónicas no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de firmar.

3. La generación o la gestión de los datos de creación de la firma electrónica en nombre del firmante solo podrán correr a cargo de un prestador cualificado de servicios de confianza.

[43] "Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 , relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE" EUR-Lex, European Union. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:32014R0910

4. Sin perjuicio de la letra d) del punto 1, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante podrán duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de los citados datos siempre que se cumplan los siguientes requisitos:

a) La seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;

b) El número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio.

A efectos prácticos, un dispositivo cualificado es un aparato (hardware) que debe poder garantizar que las firmas electrónicas realizadas con dicho dispositivo son seguras y están protegidas ante posibles falsificaciones. Para ello, estos aparatos deben poder recurrir a algoritmos criptográficos, longitudes de clave y funciones hash adecuadas.

¿Qué es un certificado cualificado de firma electrónica? Un certificado cualificado de firma electrónica, según se define en el Reglamento 910/2014 de la Unión Europea, es un certificado expedido por un prEstador cualificado de servicios de confianza, y que cumple con los requisitos de los certificados cualificados de firma electrónica establecidos en el Anexo I del Reglamento 910/2014.

Requisitos de los certificados cualificados de firma electrónica

Los certificados cualificados de firma electrónica contendrán:

*una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de firma electrónica;

*un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y

*para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,

*para personas físicas, el nombre de la persona;

*al menos el nombre del firmante o un seudónimo; si se usara un seudónimo, se indicará claramente;

*datos de validación de la firma electrónica que correspondan a los datos de creación de la firma electrónica;

*los datos relativos al inicio y final del período de validez del certificado;

*el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;

*la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;

*el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra g);

*la localización de los servicios que pueden utilizarse para consultar el Estado de validez del certificado cualificado;

*cuando los datos de creación de firma electrónica relacionados con los datos de validación de firma electrónica se encuentren en un dispositivo cualificado de creación de firma electrónica, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático.

El objetivo de los certificados electrónicos es validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta, y puede hacerlo porque contiene los datos del individuo o entidad en cuestión: nombre, NIF, algoritmo y claves de la firma, fecha de expiración y organismo que lo expide.

Para conseguir un certificado electrónico es necesario presentarse personalmente en la entidad que lo expide, para que ésta pueda comprobar la identidad de la persona que va a ser usuaria de dicho certificado. Un ejemplo clásico de certificado digital es el que está contenido en el DNI (documento Nacional de Identidad) , aunque también existen los certificados digitales que se guardan en archivos de software.

Ventajas de la firma electrónica avanzada respecto a la cualificada

Debido a los requisitos que debe cumplir una firma electrónica para considerarse como cualificada - debe ser creada mediante un dispositivo cualificado de creación de firmas electrónicas y estar basada en un certificado cualificado de firma electrónica - es difícil utilizar este tipo de firma para identificar al usuario en aquellos trámites o transacciones en los que prima la facilidad, la inmediatez y, sobre todo, la movilidad.

Hoy por hoy, la mayoría de la población no dispone ni de un dispositivo cualificado ni de un certificado cualificado de firma, por lo que requerir su uso para firmar contratos, documentos o altas de usuarios es una barrera clara que puede interrumpir el transcurso de cualquier tipo de transacción.

Por todo ello, el uso de la firma electrónica cualificada está más restringido al ámbito de la administración pública. La mayoría de empresas que utilizan la firma electrónica optan por la solución avanzada, puesto que les permite operar con total seguridad en el entorno online e identificar a sus clientes o usuarios con todas las garantías legales.

Características base de firma electrónica avanzada

*Permite identificar al firmante, puesto que recogemos una serie de datos que se asocian al mismo de forma inequívoca durante el proceso de firma: email, geolocalización, y los datos biométricos del grafo cuando el dispositivo lo permite, entre otros datos.

*Es posible detectar cualquier cambio efectuado en el documento firmado, gracias a que utiliza un sistema de clave pública/privada tanto para el documento firmado como para el documento probatorio, lo que nos permite cifrar toda la documentación generada y ello garantiza la integridad de los datos en todo momento.

*Vincula la documentación generada al firmante y a sus datos, proporcionando un sistema de hash y clave única que se relaciona directamente con el firmante.

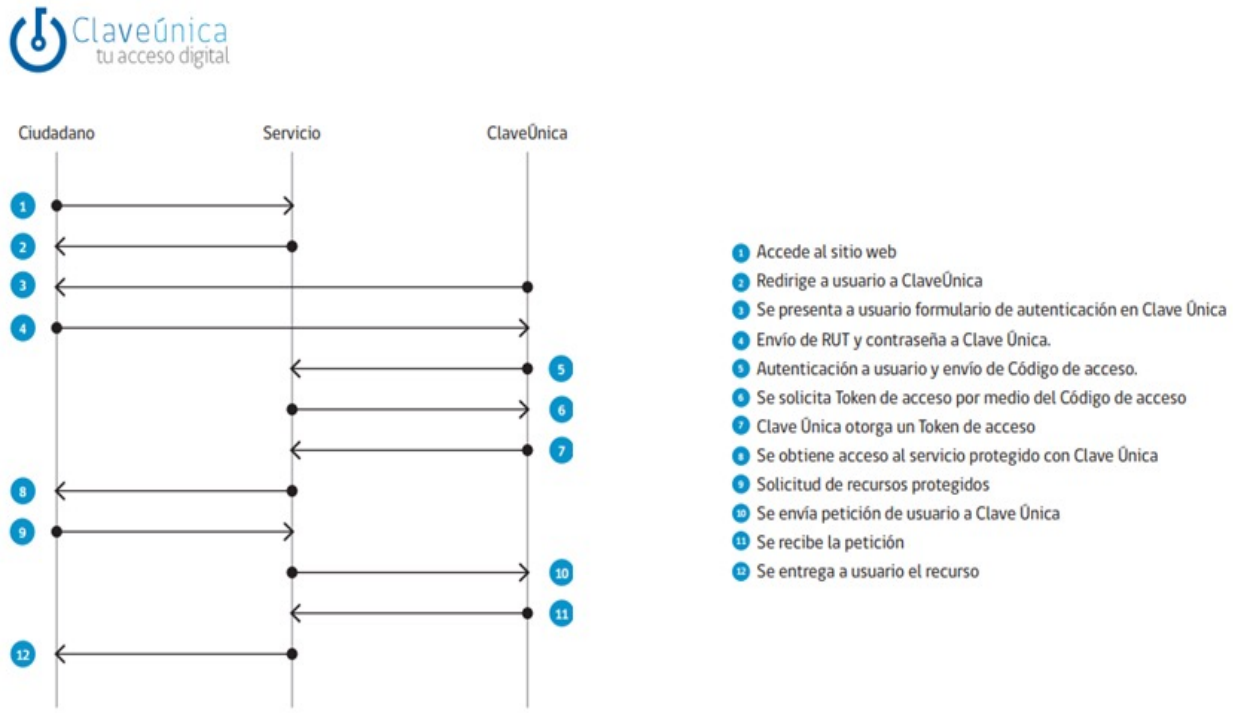
*Se crea por medios que se encuentran bajo el control del firmante: la firma se genera directamente desde el dispositivo del firmante y sólo se puede acceder a ella mediante el acceso a cuentas privadas del mismo.

6.2 Contexto nacional y casos de uso internacionales

De acuerdo con la Ley 19.477, entendemos que la identidad civil de las personas es acreditable por un órgano público centralizado llamado Servicio de Registro Civi e Identificaciónl, sin embargo, la interoperabilidad incluye además de la persona natural, a la persona legal o jurídica, y también las identidades internacionales. Más aún, la interoperabilidad integra los procesos digitales para expandir el intercambio de información entre múltiples actores locales y globales (Naser, 2020).

De este modo, las Leyes 19.799 y Ley 10.886 que regulan el uso de la firma electrónica, como la tramitación digital de los procedimientos judiciales, no están diseñadas para intercambio internacional o transfronterizo. Desde la perspectiva de la Ley 19.799, el principio de no repudio es provisto por una firma electrónica avanzada donde múltiples elementos criptográficos participan, como por ejemplo un certificado digital, llave privada y pública. Ahora bien, como se puede advertir la firma avanzada ha sido dirigida al intercambio de documentos electrónicos propios de la Administración del Estado, y así, la firma electrónica simple es implementada como mecanismo para establecer interacciones de seguridad suficientes: usuario y contraseña, o ClaveÚnica (SEGPRES, 2004; SEGPRES 2005).

El sistema de clave única está basado en la tecnología OpenID Connect, que es un protocolo estándar que permite autenticar y/o autorizar identidades para obtener un recurso protegido. Permite tres flujos para la autenticación, de los cuales se utiliza el Flujo de Código de Autorización que tras la identificación del usuario en el Registro Civil e Identificación, asocia un código de acceso que puede ser cambiado por un token lógico de acceso que tiene un tiempo de expiración. El siguiente diagrama de secuencia se resume el proceso de autenticación y autorización de ClaveÚnica:

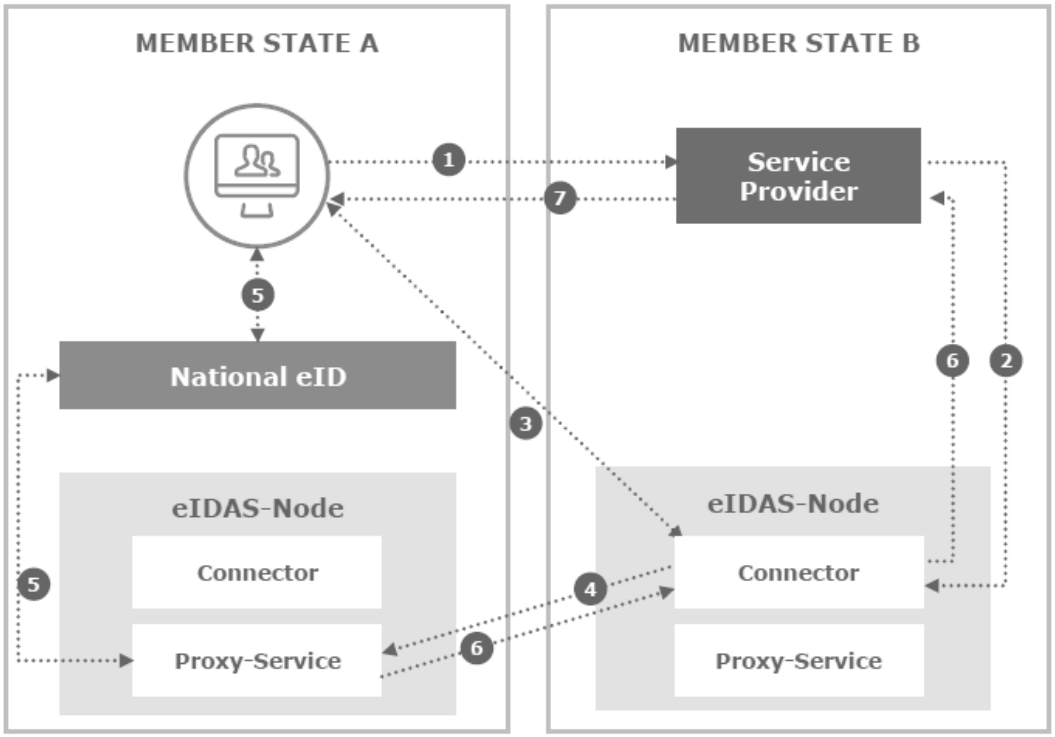


Caso Europeo

La Unión Europea (UE) es una comunidad internacional conformada por 27 Estados miembros, y que nace en 1992. La UE se funda en un modelo democrático y representativo, con poderes separados en entidades legislativas, judiciales y ejecutivas. La proyección de crecimiento del producto interno bruto de la UE es del 4.3% para 2022.

El marco de referencia de Identificación Electrónica y Servicios de Confianza, eIDAS (EU/910/2014) inicia su adopción en 2014. El objetivo de la regulación eIDAS es interoperar de manera segura entre los múltiples Estados miembros y así alcanzar los beneficios de una economía digital unificada. Para 2030, se espera que eIDAS proporcione una identidad digital para el 80% de todos los ciudadanos de la UE.

La implementación de eIDAS implica un punto único de contacto por Estado miembro (national eID), y en consecuencia, la interoperación transfronteriza ocurre en una red de nodos de eIDAS, complementariamente. Cada nodo (eIDAS-node) consiste en un conector y un servicio proxy o middleware. En la siguiente figura notamos que un ciudadano del Estado miembro A solicita un documento electrónico desde el Estado miembro B, y lo hace a cierto proveedor de servicio que debe verificar si la identidad del solicitante es legítima. El nodo asociado en la localidad B recibe la petición e interactúa con un nodo en localidad A que redirige la consulta hacia el nodo nacional correspondiente. Finalmente, es el nodo nacional el ente central y custodio de la identidad que confirma directamente con el solicitante y ciudadano que autorice la solicitud desde otro Estado miembro.



El esquema del nodo nacional eID permite el reconocimiento mutuo entre miembros, y por lo tanto, cada Estado propone un esquema en sintonía con las especificaciones técnicas definidas por la Agencia de Ciberseguridad ENISA (526/2013/EC) , y que son publicadas por el comité técnico de ETSI TC ESI. Para el 2019, el 77% de todos los países participantes implementó completamente eIDAS en su legislación nacional, en 2018 entró en rigor.

El proceso de validación de identidades establece una relación de confianza que se forja sobre una infraestructura de llave pública interoperable (PKI), que consiste en un conjunto de estándares técnicos y servicios que facilitan el uso de cifrado o criptografía asimétrica. La gestión de PKI comprende la emisión de certificados digitales, gestión de llaves, renovación y revocación de certificados, y registro de autoridad, entre otros.

El marco de referencia se acopla a la regulación de procesamiento de datos personales, para otorgar niveles de garantía o seguridad según el riesgo del dato consultado (REGLAMENTO (UE) 2016/679 Art. 32) . Este nivel (Level of Assurance, LoA) define tres niveles de identificación electrónica: Bajo, Medio o Sustancial y Alto (ISO/IEC 29115:2013).[44] La certificación de cada nivel abarca los procesos de autenticación, verificación y demostración (proofing), siendo el nivel más alto equivalente al mayor grado de certeza y credibilidad.

Finalmente, el marco legal europeo asocia a cada tipo de firma electrónica un nivel de seguridad distinto:

*firma electrónica simple: no permite identificar al firmante de forma única.

*firma electrónica avanzada: permite identificar al firmante de forma única.

*firma electrónica cualificada: permite identificar al firmante de forma única, pero es necesario disponer de un certificado cualificado de firma electrónica y de un dispositivo cualificado de creación de firma.

Debido a esta jerarquización de firmas según sus niveles de seguridad, se asume que las firmas electrónicas según la normativa europea cumplen también con las leyes Estadounidenses, siempre y cuando una ley federal norteamericana no imponga características técnicas concretas, más allá de lo definido en la UETA Act y la E-Sign Act.

Caso Estonia

Principios de identidad Estonia

→el Estado es el único responsable de identificar a las personas;

→la gestión es centralizada;

→cada persona debe contar con una y solo una identidad legal, y

→el vínculo entre el documento físico y el certificado digital es inequívoco y verificable públicamente a través de un elemento fundamental en el sistema estonio: el código de identificación personal (PIC, por su sigla en inglés), que se puso en vigor en 1992.

El PIC es un número de 11 dígitos. Contiene información personal (género y fecha de nacimiento), a diferencia de otros países donde el número de identidad es completamente secuencial y, por lo tanto, no contiene ninguna información personal. El PIC se asigna cuando la persona se inscribe en el Registro de Población.

Los sistemas o esquemas digitales de identidad se agrupan en tres tipos: de bajo nivel de seguridad, basados en infraestructura de llave pública (PKI) y blockchains.

[44] ISO/IEC 29115:2013, Joinup, Interoperable Europe. European Commission. Disponible en: https://joinup.ec.europa.eu/collection/ict-standards-procurement/solution/isoiec-291152013-information-technology-security-techniques-entity-authentication-assurance

Los sistemas de identidad digital de bajo nivel de seguridad utilizan medios como tarjetas de contraseña y calculadoras de PIN. A pesar de la inseguridad de estos esquemas, son los que predominan en el mundo digital. La autenticación de nombre y contraseña prevalece en las redes sociales. Lamentablemente, muchos países y grandes proveedores de servicios solo ofrecen esquemas de este tipo.

Los sistemas de identidad digital basados en PKI se construyen a partir de criptografía asimétrica. Se utilizan un par de llaves criptográficas: las llaves pública y privada. La clave pública es administrada por el proveedor de identidad. Los sistemas difieren en los métodos de almacenamiento de claves privadas. Los más comunes son los esquemas en los que la clave privada se encuentra en el chip de un documento de identidad digital o en una tarjeta SIM de teléfono celular (estos esquemas son los que se utilizan en Estonia). Esto asegura la protección de la clave por parte de su propietario.

Caso Canadá

En términos resumidos, los requisitos mínimos que establece el modelo de Canadá para establecer niveles de garantía de identidad son los que se muestran en el siguiente Cuadro.

Requisitos mínimos para establecer un nivel de garantía de identidad

Requerimiento	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Unicidad	o Definir información de identidad o Definir contexto			
Evidencia de identidad	No hay restricción sobre lo que se proporciona como evidencia	Un ejemplo de evidencia de identidad	Dos casos de evidencia de identidad (al menos uno debe ser una prueba fundamental de identidad)	Tres casos de evidencia de identidad (al menos uno debe ser una prueba fundamental de identidad)
Precisión de la información de identidad	Aceptación de la autoafirmación de la información de identidad por parte de un individuo	La información de identidad coincide aceptablemente con la afirmación de un individuo y la evidencia de identidad, y Confirmación de que la evidencia de identidad proviene de una autoridad apropiada	o La información de identidad coincide aceptablemente con la afirmación de un individuo y de todos los casos de evidencia de identidad Y, o Confirmación de la evidencia fundamental de la identidad, utilizando una fuente autorizada, y o Confirmación de que la evidencia de identidad de apoyo proviene de una autoridad apropiada, utilizando una fuente autorizada Siempre que no se pueda aplicar nada de lo anterior:	
			o inspección por parte del examinador capacitado	
Vinculación de la información de identidad con la persona	Sin Requerimiento	Sin Requerimiento	Al menos uno de los siguientes: o confirmación basada en el conocimiento o confirmación biológica o de características de comportamiento o confirmación del árbitro de confianza o confirmación de posesión física	Al menos tres de los siguientes: o confirmación basada en el conocimiento o confirmación biológica o de características de comportamiento o confirmación del árbitro de confianza o confirmación de posesión física

6.3 Criterios de un Sistema de Identidad Digital

Sabemos que una firma digital es derivada de mecanismos criptográficos que son aplicados al contenido de un mensaje o documento para demostrar al receptor del mensaje que el emisor del mensaje es real (autenticación), que éste no puede negar que envió el mensaje (no repudio) y que el mensaje no ha sido alterado desde su emisión (integridad).

La firma digital es por tanto una parte fundamental de la firma electrónica avanzada y de la firma electrónica cualificada, pero no de la firma simple.
La firma digital también es legal, aunque no tiene naturaleza jurídica, en el sentido de que su objetivo no es dar fe de un acto de voluntad por parte del firmante, sino tan sólo en cifrar los datos de un documento para conferirle mayor seguridad.

Con el advenimiento de la economía digital, las interacciones y transacciones que hasta ahora solo se realizaban en forma presencial están empezando a ejecutarse a través de sistemas de información interconectados. De allí surge la necesidad de tener en cuenta la identidad digital de cada persona para que se identifique y sea autenticada, obtenga los permisos para acceder a determinados recursos de información o físicos (por ejemplo, el acceso a un área) y realice transacciones a través de Internet o redes privadas.

En la economía digital es necesario identificar a las personas a distancia, sin mediar una interacción física, en la mayoría de los casos sin conocimiento previo de la otra parte y muchas veces siendo una computadora la encargada de ejecutar el proceso. Como consecuencia, la gestión de la identidad conlleva, por un lado, desafíos en cuanto a privacidad, protección de datos y nuevos riesgos de fraude y, por el otro, la necesidad de revisar y ajustar esquemas de gobernanza, marcos legales y tecnologías que puedan estar quedando obsoletas.

La identidad digital puede clasificarse en dos categorías:

*Identidad digital legal: es la que requiere estar vinculada a la identidad legal de una persona física o jurídica. Es necesaria, por ejemplo, para realizar transacciones con el gobierno o con instituciones financieras reguladas.

*Identidad digital simple: es aquella que no requiere estar vinculada a una identidad legal física. Se utiliza, por ejemplo, para conectarse a redes sociales.

Identidad Digital Legal

Se plasma en lo que se conoce como documentos de identidad fundamentales (certificados de nacimiento para ciudadanos naturales, registros de inmigración para ciudadanos legales o residentes, o documento nacional de identidad en ambos casos). A partir de estos documentos se pueden generar los documentos de identidad funcionales (pasaporte, licencia de conducir, etc.) y las identidades digitales legales.

Una de las formas más usuales de identidad digital es un nombre de usuario. En el caso de la identidad digital legal, es este nombre de usuario el que está vinculado a una identidad física. La vinculación se produce en el momento del enrolamiento.

Todo sistema de identidad cuenta con tres tipos de actores básicos (Deloitte, 2016):

*los usuarios de servicios, quienes obtienen una identidad a efectos de cumplir con la normativa y poder realizar transacciones;

*los proveedores de identidad, quienes capturan y almacenan los atributos de la identidad de los usuarios, se aseguran de que sean verdaderos y llegan a completar transacciones en nombre de estos, y

*los proveedores de servicios (básicamente, las empresas y el gobierno), quienes se apoyan en los proveedores de identidad a efectos de cumplir con el requerimiento KYC (del inglés "know your customer", que podría traducirse como "sepa quién es su cliente"), en todos aquellos casos en los que las buenas prácticas lo aconsejen o la normativa lo requiera.

Gestión de Sistemas de Identidad

Combina procesos y tecnologías que potencian el uso de los datos identificatorios de las personas, y requiere:

*un modelo de gobernanza y un modelo de negocio;

*un marco legal apropiado y actualizado;

*la simplificación y estandarización de procesos y sistemas;

*el establecimiento de mecanismos de interoperabilidad que faciliten la coordinación entre los diferentes organismos,

*y la promoción y coordinación del ecosistema de uso de la identidad.

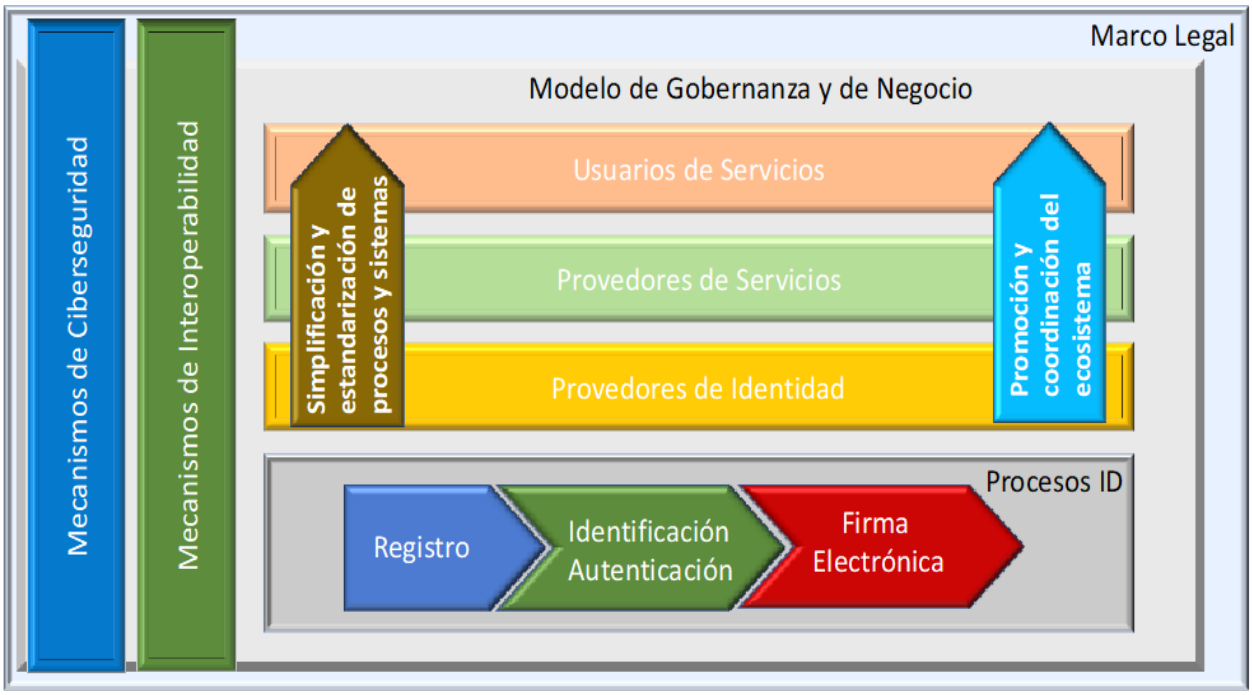
Procesos de Sistemas de Identidad

***Registro en un sistema de identidad digital.** Se crea un usuario del sistema y se le asigna una credencial digital. El enrolamiento puede ser presencial o en línea. En el primer caso, se suele firmar un compromiso de responsabilidad por el uso de la identidad digital. En el segundo caso, es común incluir un paso de confirmación a través de un enlace o una clave enviados al correo electrónico o teléfono del usuario.

***Identificación y autenticación.** Tiene lugar cuando se intenta acceder a algún sistema de información. Las personas se identifican mediante una credencial física o digital y, mediante la autenticación, se verifica que la persona sea quien dice ser.

***Firma electrónica.** Es un mecanismo informático que permite demostrar la autenticidad de un documento o mensaje.

Gestión de Sistema de Identidad Digital



La autenticación es un proceso clave en el mundo digital. Históricamente se ha sustentado en tres elementos (factores) que se utilizan para mejorar la robustez y seguridad del método, a saber:

*Algo que la persona sabe: una clave o la respuesta a una pregunta personal.

*Algo que la persona es: biometría dactilar, de iris, cara o voz.

*Algo que la persona tiene: una tarjeta de identidad o de crédito, un certificado digital.

Un certificado digital es un archivo digital que en el mundo digital cumple funciones similares a las de una tarjeta de identidad física que incluye la firma de la persona. Por lo tanto, el archivo contiene la identificación de la persona y su clave pública. Es parte del mecanismo que puede utilizar su dueño para firmar paquetes de información (documentos).

Las buenas prácticas señalan que, para operaciones de riesgo alto, se debe utilizar una combinación de al menos dos de estos elementos. Entre las más recientes novedades en autenticación se puede mencionar, para algunos servicios en línea, la adopción de mecanismos complementarios de seguridad de tipo adaptativo, basados en la historia de los usuarios (su perfil de navegación, geolocalización, perfil de uso de redes sociales, etc.).

Las firmas digitales se realizan a través de certificados digitales y permiten no solo dar consentimiento al contenido de un documento o mensaje sino asegurar su inviolabilidad y el no-repudio de la firma.

En el sector público de America Latina y el Caribe, el grado de desarrollo de las transacciones en línea es muy bajo. Entre los principales factores causales de este bajo nivel de desarrollo se pueden mencionar:

*las escasas posibilidades de uso de los certificados, debido a la baja oferta de servicios que aceptan firmas digitales y al relativamente reducido número de casos de uso donde es necesaria una firma digital con certificado;

*el costo para el usuario (considerable en sus comienzos);

*la incomodidad que le representa al usuario tener que contar con un lector del dispositivo donde se almacena el certificado (smartcard, token-USB u otro), y

*varios marcos normativos que pueden haber sido aprobados para emular a países avanzados, siguiendo una moda, más que teniendo en cuenta la situación local o manejando con realismo las expectativas de adopción.

Costos Identidad Digital

Los principales componentes del costo de gestión de la identidad digital son los siguientes:

*Implementación y mantenimiento del soporte tecnológico, constituido por bases de datos, la plataforma PKI (por su sigla en inglés, Public Key Infrastructure), el software de gestión de los datos de identidad y otras medidas de ciberseguridad.

*Enrolamiento y revocación de certificados. Debido a su criticidad, en muchos casos es un trámite presencial, con el consiguiente alto costo tanto para la institución como para los ciudadanos.

*Adquisición y mantenimiento de dispositivos que almacenan certificados (tokens, tarjetas, lectores, generadores de claves dinámicas, etc.).

*Soporte a usuarios (por ejemplo, cuando olvidan su clave).

6.4 El caso chileno

Chile posee un mecanismo de identificación nacional de ciudadanos y personas jurídicas basado en el RoI Único Nacional (RUN) y RoI Único Tributario (RUT), definido a principios de la década de 1970. El modelo de operación contempla que la asignación y administración de RUNs corresponde al Servicio de Registro Civil e Identificación (SRCeI), y en el caso del RUT, al Servicio de Impuestos Internos (SII).

El modelo en general es una fortaleza del país, ya que permite un mecanismo de identificación multisistema, utilizado en múltiples industrias, siendo parte del día a día del país. Si bien facilita la identificación de los ciudadanos tanto en las operaciones del mundo público como privado, posee algunos aspectos que requieren una mejora, en cuanto a su aplicación y extensión.

Algunos aspectos que requieren una mejora al mecanismo nacional de identificación corresponden:

*Los números no son reutilizables, lo cual puede generar en problemas de disponibilidad futura (revisar disponibilidad y modelo de distribución entre instituciones).

*Hay desafíos en relación con la privacidad, tema que se contempla en propuestas legislativas en discusión en el parlamento, relacionadas con la Ley de Protección de Datos Personales.

Modelos de Autenticación

Producto de la creciente utilización de servicios digitales sobre Internet, los diversos proveedores de servicio tanto públicos como privados han debido incorporar mecanismos de identificación (en muchos casos basados en el Identificador Nacional, el RUN/RUT) y clave secreta, en un modelo de autenticación basado en un factor (clave secreta).

En algunas industrias y servicios públicos, se han extendido estos modelos de autenticación hacia modelos basados en el identificador nacional (RUN/RUT) y dos factores (clave secreta y token, clave secreta y biometría, clave secreta y teléfono móvil). No obstante, todos los mecanismos son propietarios de la institución que presta el servicio y con modelos de enrolamiento y administración propios.

En el caso del sector público, el Estado de Chile ha desarrollado un modelo de autenticación único llamado Clave Única, que está siendo incorporado en todos los servicios del Estado, con aproximadamente 14 millones de ciudadanos activos a esta fecha. El servicio se pone a disposición del mundo público, sobre la base de la identidad certificada por el Servicio de Registro Civil e Identificación y operado por la División de Gobierno Digital de la Secretaría General de la Presidencia.

A la fecha, sigue un modelo de autenticación monofactor (clave secreta), integrado tecnológicamente en un modelo OpenID 2.0.

Clave Única ha mostrado ser un importante apoyo para la implementación de trámites en la relación con los ciudadanos, especialmente en su relación con el Estado, permitiendo además la implementación de trámites con respaldo legal. Hasta el momento, el uso de Clave Única por parte de operadores privados que aprovechan los servicios de Clave Única es muy incipiente, aún cuando no existen restricciones técnicas para su uso.

Las situaciones antes descritas explican, por tanto, la existencia de múltiples mecanismos de autenticación propios por industria y organización (público o privado), no conectados.

Esto significa para los usuarios la obligación de administrar múltiples "identidades digitales" y "mecanismos de autenticación". En particular, una hipótesis a validar corresponde a verificar si la extensión o profundidad del uso de los servicios digitales en Chile, se ve dificultada por la operación y extensión de estos mecanismos de autenticación. Y, por cierto, el tener que administrar múltiples identidades digitales hace que se comprometan algunos criterios de seguridad (unicidad de las claves, no repetición, actualización periódica, etc.)

Identidades "no oficiales" para "no chilenos"

Siendo el RUN/RUT el identificador básico para personas en los diversos sistemas en operación en Chile, existen industrias que, por sus necesidades propias de operación, han generado "workarounds" o procedimientos de excepción, para responder a un problema de disponibilidad de un identificador nacional (RUN/RUT) para personas que no poseen dicho identificador oficial. Esta situación corresponde a personas no nacidas en Chile (ya que el modelo actual en operación hace que toda persona nacida en el territorio nacional automáticamente es asignada con un RUN por parte de SRCeI).

Ejemplos de estas industrias:

→**Educación pública:** Asigna "RUNs temporales" a hijos de inmigrantes que hacen uso del sistema nacional de educación pública.

→**Salud pública:** Asigna "RUNs temporales" a personas no chilenas que requieren hacer uso de los servicios públicos de salud.

→**Previsión Privada:** Asigna "RUNs temporales" a personas que trabajan sin obtener aún su RUN/RUT chileno y que requieren un identificador para la asignación de sus fondos previsionales.

Adicionalmente, existe un requerimiento específico de Policía de Investigaciones y servicios relacionados con inmigración y extranjería, quienes han identificado y declarado la necesidad de tener mecanismos de identificación y control de visitantes temporales a Chile.

Necesidades generales

Dados los antecedentes, se identifica por tanto una necesidad nacional de una Estrategia Nacional de Identificación que permita, tanto para la operación tradicional como para las operaciones de la economía digital, mecanismos que resuelvan necesidades en dos niveles:

→ Identificación (que pueda ser utilizada por múltiples sistemas)
→ Autenticación (que pueda ser compartida entre múltiples actores)
→ Experiencia usuaria simple
→ Diversos niveles de seguridad
→ Opciones multifactor (dos o más factores)
→ Interopere entre múltiples industrias
→ Compatibles con el Modelo Nacional de Identificación

Adicionalmente, sobre la base de casos de uso internacional, se considera necesario analizar con detalle casos de uso en los cuales se justifique extender las capacidades tecnológicas de identificación y almacenamiento contenidas en la Cédula Nacional de Identidad. Por ello, es necesario definir un Modelo de Identificación Nacional Único. Junto a ello, existe un consenso respecto a que la base del modelo de identificación chileno y repositorio de la fe pública en la gestión de identidades, es el Servicio de Registro Civil e Identificación.

No obstante, se requiere diseñar un modelo de "Identidad Digital" que lo complemente, resuelva en forma homogénea y consistente los requerimientos de diversas industrias y que resuelva las necesidades del ecosistema nacional, tanto de los actores públicos como privados.

Adicionalmente, el modelo de "Identidad Digital" debe incorporar un modelo de autenticación que permita su uso en forma extendida por múltiples industrias, en un modelo de colaboración.

Una buena opción de implementación del mecanismo nacional de autenticación es extender el modelo de Clave Única, incorporando mecanismos multifactor (dos o más factores). Para ello, se recomienda explorar los modelos de Estonia, España y Uruguay.

Para aquellas industrias que no hayan aún implementado aún mecanismos de autenticación en sus sistemas se propone además la extensión del uso de este modelo de Clave Única al menos para implementar niveles de servicio básicos, restringiendo el modelo de responsabilidad del Estado (sobre las operaciones).

Necesidad de un Modelo de Gobernanza Nacional

Dados los criterios previos, el principal tema a resolver corresponde a diseñar un modelo de Gobernanza Nacional de Identidad Digital, que defina:

→Quién (es) administran
→Quién (es) lo usan, dando autoridad a quién (quiénes)
→Cuál es el nivel de responsabilidad
→Cuáles son los estándares tecnológicos que lo sustentan
→Cuál es la infraestructura base que lo soporta
→Quiénes aportan, financian y operan dicha infraestructura

Extensión del uso de la Cédula Nacional de Identidad

Como parte del modelo de Gobernanza Nacional de la Identidad Digital, se propone la creación de un espacio específico de discusión sobre el uso de la Cédula Nacional de Identidad, y que se contemplen estas definiciones en las nuevas bases de licitación del sistema de identidad del Servicio de Registro Civil e Identificación.

Algunos aspectos que pueden ser considerados en este espacio de discusión son:

→Emisión de "Cédulas Temporales" de Identificación
→Explorar el uso del Chip como un Wallet Personal
→Potenciales fraudes que puedan ser realizados mediante la inhabilitación de mecanismos de seguridad y manejo de excepciones

7. GENERACIÓN DE VALOR POR LA INTEROPERABILIDAD E IDENTIDAD DIGITAL

7.1 Consideraciones para criterios técnicos

La prestación de la gran mayoría de los servicios públicos requiere que diferentes órganos del Estado colaboren para satisfacer las necesidades de los usuarios finales en la prestación de servicios de manera integrada. Para estos efectos los servicios deben tener una gobernanza operacional que garantice esta integración, la continuidad del intercambio de información en forma ininterrumpida, la reutilización de servicios y datos y el desarrollo de nuevos servicios.

La gobernanza a nivel organizacional en que los procesos institucionales que intercambian información, servicios y componentes en que se sustenta la prestación del servicio integrado, debe definirse de acuerdo a legislación, necesidades de usuarios y nuevas tecnologías. En esta la estructura organizativa de los procesos y sus tecnologías habilitantes, se deben incorporar acuerdos formales en temas como los niveles de servicios sobre interoperabilidad, procedimientos de gestión de cambios, planes de continuidad operacional, y la calidad de los datos.

Los Criterios Técnicos para generar la tecnología que soporte interoperabilidad del Estado se describe a continuación:

Infraestructura Basal:

a)Determinar los requerimientos computacionales de las organizaciones del Estado para poder manejar e intercambiar información

b)Medición si la infraestructura informática de la red del Estado se encuentra capacitada para soportar servicios interoperables

*Servicios disponibles
*Red de Datos Habilitada
*Ancho de banda y Calidad de Servicio

c)Consideraciones sobre el tipo de Arquitectura (cómo se conforma la red de servicios digitales del Estado

*Centralizada, Distribuida, Federada
*Nube, Servidores por Organización, etc

b)Derechos de propiedad sobre los servicios del Estado a nivel normativo
*bien público (desarrollos propios)
*licencias
*Sistema Llave en mano/ propietarios

Infrestructura: Consideraciones de los basales estratégicos para interoperar

c)Estandarización: Definición de estándares a usar

*Estándar Sintáxtico
*Estándares semánticos (tesauro, taxonomía estándar)
*Estándares Organizacionales.

e)Levantamiento de Habilitantes

*Servicios de Terminologías
*Servicios de Identificación de Objetos y sus modelos (OID : Object Identifier)
*Repositorios para servicios específicos definidos en la oferta de valor
*Servicios de Identificación General

Lo anterior implica tener que contar con una definición y criterio para determinar una de las dos opciones:

1)Criterios para adjudicar una única plataforma de interoperabilidad
2)Criterios para definir las normativas para que los desarrollos o compras de sistemas locales interoperen en base a estándares y arquitecturas definidos

f)Generación de un modelo de actualización de los criterios técnicos

7.2 Modelo de generación de Valor

La concepción de un Estado moderno en donde sus procesos sean informatizados y la información que se requiera desde una unidad a otra pueda ser disponibilizada para la mejora en la eficiencia de los procesos, tanto a nivel interno como para favorecer la gestión de requerimientos que la población debe ejecutar. Lo anterior genera valor en varias dimensiones que son aquellas que nombramos a continuación:

a)Valor público: Los servicios que da el Estado se ven favorecidos en diferentes aspectos, destacando por sobre todo los siguientes:

***Eficiencia:** El Estado mejora la capacidad de ejecutar los procesos, dado que el flujo de información es continuo. Esto posibilita una mejor capacidad para tomar decisiones oportunas, ahorro de tiempo en la búsqueda, recopilación y análisis de la información, y acortar los tiempos de espera servicios, tanto para usuarios del Estado como para la ciudadanía

***Calidad:** La calidad se puede medir en dos dimensiones: Calidad en el manejo de la información (del dato); calidad en el servicio que se entrega. Interoperar permite evitar la duplicidad de datos, la doble o triple tabulación la transcripción de información lo cual produce error natural y daño de la información. Por otra parte, contar con servicios que tienen información oportuna y sin errores mejora la calidad de los procesos y por lo tanto de los servicios que el Estado brinda

***Satisfacción Ciudadana:** La satisfacción se refiere al impacto ex post obtenido la respuesta a su requerimiento. Otra forma es evaluar la percepción del usuario en el viaje de su solicitud. A la ciudadanía le interesa no perder tiempo navegando por diferentes servicios del Estado para buscar información que le haga concretar un único trámite. Además, la pérdida de continuidad de los procesos que son parte de los servicios del Estado perjudica notoriamente la percepción en como un ciudadano percibe la calidad de los servicios del Estado. Interoperar acorta los tiempos de procesos y hace que el viaje del ciudadano ante el requerimiento de un servicio sea más simple y corto mejorando la percepción de satisfacción.

b)Impactos Sociales

*Cohesión y equidad: La OCDE (2014), define que los beneficios que la sociedad puede ver según la perspectiva de los diferentes actores son el valor público que entrega como resultado el ejercicio de ciertas estrategias del Estado. Uno de estos valores al momento de interoperar el Estado es el de equidad y cohesión social, pues permite que la eficiencia del Estado llegue a toda la población de manera igualitaria, bajando los costos de los trámites, percibiendo un Estado más justo

*seguridad y confianza: Al hacer disponible la información de manera interoperable, se empieza a garantizar el principio de transparencia, se hace más complejo no informar y es más simple cotejar la información, pues esta se puede obtener de diversas fuentes. El Estado se hace más transparente en sus procesos y ante la ciudadanía

c)Confianza y legitimidad: Uno de los desafíos del Estado es lograr legitimarse ante la población. La seguridad y transparencia como objeto de valor para el Estado acarrea la generación de confianza y legitimidad por parte de la población, lo que permite de manera indirecta mejorar la calidad de vida d la población y avanzar política y socialmente en estrategias más legitimadas por la ciudadanía.

d)Valor Percibido por la población: Para la población el valor se manifiesta en los siguientes elementos, que son más cualitativos que cuantitativos.

*Reducción de costos y mejor organización para los servicios a las personas
*Mayor transparencia
*Facilidad de mantenimiento y evolución tecnológica
*evolución tecnológica más organizada

7.3 Propuesta para Generar Modelo de Valor

Considerando los informes emitidos por las siguientes entidades CEPAL, "Gobernanza Digital e Interoperabilidad Gubernamental", Alejandra Naser; OCDE; Homeland Security, "Communications Interoperability Performance Measurement Guide", 2018; Ministerio Secretaría General de la Presidencia, "Estudio de Caracterización de la Interoperabilidad en el Estado de Chile", 2017; BID (Banco Interamericano de Desarrollo) (2019), El ABC de la interoperabilidad de los servicios sociales: marco conceptual y metodológico [en línea]; Comisión Europea (2020), "The Digital Economy and Society Index (DESI)"

Se propone el modelo de valor indicado por la CEPAL en divisiones del modelo CANVAS

Modelo Canvas de División, para valor de interoperabilidad. (Fuente: "Gobernanza Digital e Interoperabilidad Gubernamental, CEPAL)

El modelo gira en torno a determinar la propuesta de valor que no necesariamente es todo lo que se puede alcanzar interoperando, sino que algún objetivo puntual que el Estado determine.

El modelo debe basarse en que esta propuesta parte del hecho que cada organización que pertenece al Estado debe definir su propuesta de valor institucional, que debe estar basada en las funciones que ejerce, y que son ponderadas por las directrices del gobierno.

Luego la propuesta de valor debe ser matizada de forma tal que cumpla

1)Comprensión por parte de la ciudadanía de esta

2)Identificación de los servicios o productos estratégicos

3)Claridad en los procesos y en donde se debe generar transformación tecnológica

4)Estructura organizacional acorde.

Si a lo anterior se le adhiere los mecanismos para que esa propuesta de valor institucional se robustezca alineada con la de las demás organizaciones que conviven en el ecosistema del Estado, la interoperabilidad cobra relevancia y aporta al valor del gobierno digital

7.5 Indicadores de Medición

La experiencia europea, indica lo crítico de desarrollar indicadores de medición dentro de la normativa local. En dicha experiencia se determinan los siguientes tipos de indicadores:

1)Indicadores de Performance: Indican el desempeño de las estrategias de interoperabilidad (Entradas, Procesos, salidas, resultados e impactos)

2)Indicadores de Capacidades: Permiten medir si la implementación de interoperabilidad es realizable o no

3)Indicadores de Rendimiento: Básicamente Técnicos permiten determinar si la data recolectada es usable o no

8- GESTIÓN DEL CAMBIO: EJE DEL ÉXITO

En todo proceso de cambio organizacional y, en especial asociado a aquellos que incorporen componentes tecnológicos, existen barreras para lograr éxito en esta transformación, es por ello que es necesario hacerse cargo de estas barreras, analizarlas y realizar acciones tendientes a evitarlas.

Así como también es necesario identificar los facilitadores del cambio, aquellos rasgos, características, personas, y/o situaciones de la o las organizaciones que pueden permitir acelerar o instalar el cambio que se desea. La mayoría de estas barreras o fuerzas de resistencia provienen de las personas o de la cultura organizacional.

Mediante una Estrategia de Gestión del Cambio que se operacionalice a través de un Plan de Implementación de acciones es posible contribuir a disminuir esta resistencia y potenciar a los facilitadores para crear condiciones más propicias para la implantación de proyectos de Gobierno Digital, Interoperabilidad, Identidad Digital y Ciberseguridad. Esta estrategia debe cubrir tanto a los actores de las instituciones gubernamentales, empresas y ciudadanía, de tal forma de impulsar un cambio cultural ad hoc a esta nueva forma digital de relacionarse entre los distintos actores del país.

Las organizaciones normalmente realizan ajustes en términos de las personas, reenfocando, capacitando e integrando nuevos recursos que cumplan con las competencias requeridas para manejar, administrar y dominar un cambio como el asociado a la implementación de la Transformación Digital del Estado que derivara en un Gobierno Digital.

La comunidad de ciudadanos es más exigente y las trabas no están en la tecnología ni en su funcionalidad, está en las prácticas y la cultura que esta tiene, por tanto, es desde allí donde se debe trabajar.

45 https://www.cisa.gov/sites/default/files/publications/Communications%2BInteroperability%2BPerformance%2BMeasurement%2BGuide_0.pdf

8.1 Necesidad de la Gestión del Cambio

La Gestión del Cambio tiene como centro al factor humano. Su permanente seguimiento, valoración y la mejora en la calidad motivacional, genera una de las ventajas competitivas más fuertes en cualquier industria.

El objetivo implícito de la Gestión del Cambio es hacer participar cada vez más al personal de la Organización en todo el proceso de transformación, mantener el nivel de adhesión y aumentar el nivel de involucramiento, facilitando la definición de las mejores soluciones para la materialización del Proyecto y logrando la asimilación de las mejoras que éste traerá aparejado.

En definitiva, con la Gestión del Cambio se logra reducir el riesgo de fracaso; acelerar la realización de los beneficios; y asegurar la sustentabilidad del cambio en el tiempo.

La sinergia entre la estrategia de la organización y su capacidad de cambio marcan la diferencia entre los proyectos exitosos y los fracasos.

Es posible sostener que las destrezas son centrales en el vertiginoso mundo que nos toca vivir y constituyen la manera de traducir los conocimientos en acciones efectivas. La construcción de confianza en los equipos de trabajo junto al manejo eficiente de redes y compromisos, son aspectos medulares para asegurar el aumento de valor.

Uno de los aspectos relevantes a tener en cuenta en un proceso de cambio es la resistencia al cambio no es intrínsecamente negativa, es una predisposición natural de los seres humanos a moverse dentro de la seguridad que brinda lo conocido.

La resistencia al cambio es una relación entre la calidad de la propuesta y las características de los afectados por ella. Sólo nos resistimos al cambio cuando lo interpretamos como una mezcla donde priman las amenazas con respecto de las oportunidades.

Hay una responsabilidad importante a desarrollar y es hacer ver oportunamente a los involucrados, las ventajas que trae el cambio a experimentar.

8.2 Antecedentes para una Gestión de Cambio Exitosa

Interacción

En todo proceso de cambio interactúan distintos actores, los que cumplen distintos roles que deben ser considerados en el diseño. Entre éstos destacan los siguientes:

*Los patrocinadores del cambio. Sus responsabilidades son evaluar las consecuencias de la transición; identificar los requerimientos adaptativos; y decidir sobre cambios por implementar.

*Los agentes de cambio. Son los encargados de administrar el proceso de cambio; conformar el equipo responsable y manejar las distintas variables del cambio.

*El personal afectado por el cambio. Estos son los que experimentan y vivencian cambios en conocimientos, actitudes y conductas.

Aspectos claves

Desde el punto de vista de componentes, la gestión del cambio en proyectos de modernización asociados a Gobierno Digital, involucran cinco elementos considerados clave que deben estar presentes en una estrategia de gestión del cambio, a saber:

*Visión Comunicada: en relación con cuáles son los argumentos de fondo de este cambio (modernización, foco en el ciudadano, atención a distancia, valor público en el servicio, otro).

*Destrezas Entrenadas: que el universo de actores involucrados en el cambio (interno como ciudadano) cuenten con las habilidades y conocimiento suficiente y el entrenamiento requerido para hacer uso de la resultante del cambio.

*Recursos: que existan los medios económicos, personales y de infraestructura requeridos para la correcta implementación y uso del cambio.

*Incentivos: que exista una motivación asociada, que se traduzca en algún reconocimiento, no necesariamente financiero hacia el equipo y los ciudadanos involucrados (en este último caso, mayores horarios de atención, mayores plazos para rendir o menores plazos en recuperar, entre otros).

*Plan de Acción: que establezca claramente las actividades, hitos, responsables y productos asociados al proyecto de implementación.

El no contar con alguna de estas componentes, genera algún grado de impacto a nivel de las personas involucradas

Cambio en la cultura funcionaria

A nivel gubernamental, con el Gobierno Digital, se habla de un cambio cultural en los servicios públicos y sus funcionarios, en términos de:

*Poner al ciudadano como centro.
*Colaborar con otros Servicios Públicos
*Generar nuevas capacidades
*Tomar conciencia y hacerse cargo de que las labores internas y desempeño afectan a otros (los ciudadanos)
*Modificar la manera de trabajar y de relacionarse con otros para este fin

Desde la dimensión cultural, es decir desde la dimensión de las personas, significa cambios en las prácticas de trabajo, un hacer las cosas de otro modo. Este aspecto debe ser tenido en cuenta como un elemento más del plan de gestión del cambio dada su magnitud y efecto sobre la organización y su entorno inmediato.

La gestión del cambio se debe abordar desde tres perspectivas y/o pilares clave:

Impacto Organizacional (Contención)

Evaluar el nivel de impacto que tendrá una iniciativa tecnológica requiere identificar los factores que obstaculizarán y/o facilitarán el cambio, así como los impactos que tendrá para la(s) organización(es) y las personas su implementación.

Se plantea la necesidad de seguir los siguientes pasos para obtener un buen Diagnóstico de situación:

1.**Identificación del grupo objetivo:** incluye la segmentación de públicos impactados por el proyecto de cambio, sus Stakeholders y el nivel directivo, establecimiento de compromisos con la contraparte que lleva el proyecto de cambio. Se busca, además, identificar a aquellas personas que puedan constituirse en agentes de cambio del Proyecto.

2.**Evaluación del clima y cultura organizacional:** incluye la realización del diagnóstico de la(s) organización(es), comprensión del Problema, conocimiento organizacional y relevamiento de los motores del cambio, aplicación de instrumentos de medición de Clima Laboral, entrevistas, focus group para determinar el punto de partida desde lo cultural.

3.**Evaluación y relevamiento de requerimientos y brechas:** Análisis de la información generada por el proyecto de cambio para comprender las brechas existentes en la organización entre lo que expone el proyecto y la realidad de la(s) organización(es), empresas y ciudadanía, en términos de procesos, personas (roles y perfiles) y de la tecnología. Identificación de nuevos roles y competencias necesarias para el personal hacia la nueva institucionalidad identificada por el proyecto de cambio.

4.**Identificación de las barreras internas para el cambio**, así como las habilidades y competencias (presentes y ausentes) requeridas en el equipo que está llevando a cabo el proyecto de cambio, para provocar el cambio estratégico y tecnológico deseado.

5.**Identificación de los factores externos** que pueden facilitar o dificultar, el desarrollo de la estrategia de cambio a implementar en la Organización. Ciclos políticos, cambios en las direcciones de las instituciones clave.

6.**Identificación de los facilitadores y detractores** que pueden apoyar o dificultar, el desarrollo de la estrategia de cambio a implementar en la Organización. Clave es identificar nivel de impacto e influencia en los facilitadores/detractores del cambio por el proyecto,

7.**Generación de acciones de contención** (detractores) y de fomento (facilitadores).

Transferencia de Conocimiento (entrenamiento)

Se considera a las personas como el principal agente de cambio. Si se desea que ellas piensen, sientan y hagan algo de manera distinta, hay que hacerse cargo del temor, escepticismo, inseguridad, desconfianza, resistencia, ambición y desconcierto que pueden surgir en los funcionarios de las instituciones participantes y de los usuarios/beneficiarios de los servicios de dichas instituciones ante lo desconocido. En este sentido, el ámbito de transferencia de conocimiento no sólo se debe hacer cargo del conocimiento técnico asociado a las nuevas herramientas y procesos, sino que de las componentes adaptativas que involucra el cambio.

Este ámbito da cuenta, a partir del diagnóstico anterior, de las necesidades de adquisición de nuevos conocimientos, habilidades y destrezas por parte de las personas impactadas por el Proyecto Gobierno Digital.

El enfoque metodológico impulsado debe estar centrado en el "Saber Hacer" y en el "Aprender Haciendo".

Comunicación y Difusión

Éstos deben favorecer el involucramiento adecuado de todos los stakeholders en el proyecto (internos y externos) y necesariamente deben propiciar que los cambios buscados tengan cabida en los procesos y funciones que se impactarán. Lo anterior es especialmente relevante cuando se plantea un cambio tecnológico que conlleva cambios conceptuales y de prácticas.

Se debe formular e implementar un Plan de Comunicaciones y de difusión del proyecto que, debe contar con al menos los siguientes componentes:

*Identificación de stakeholders y construcción de Matrices de Tratamiento comunicacional (estrategia)
*Segmentación de stakeholders
*Definición de Contenidos (relato) para cada grupo objetivo
*Mediatización de Contenidos
*Diseño, definición y habilitación de canales de comunicación.
*Definición de la Estrategia de Gestión de los Riesgos.
*Diseño del Plan de Comunicaciones
*Ejecución y Control del Plan de acuerdo con los Gatillos de Cambio.

Cada uno de estos componentes (Contención, Entrenamiento y Comunicación) deben ser abordados en conjunto y como complementos desde la concepción de los proyectos de cambio.

Dentro de las resistencias que se presentan frecuentemente en las personas ante procesos de cambio, se identifican al menos tres categorías de grupos de personas, que configuran, a su vez, tres Pilares de Gestión del Cambio:

***Quienes no saben,** que viene un cambio y en qué consiste, por tanto hay una resistencia por desconocimiento. Para estas situaciones es que se define el **Plan de Difusión y Comunicación.**

***Quienes no quieren el cambio**, son aquellos que se oponen por alguna razón de tipo personal, profesional, política, cultural u otra, manifiestan su disconformidad, descontento y no apoyarán. Para estas situaciones es que se define el **Plan de Contención y Seguimiento de casos.**

***Quienes no pueden**, básicamente por la falta de conocimiento, competencias, habilidades. Para estas situaciones es que se define el **Plan de Formación y entrenamiento.**

8.3 Consideraciones para una Gestión de Cambio exitosa

El factor de éxito para introducir una transformación digital exitosa, en la que la Interoperabilidad y la Identidad Digital son claves radica, más que en las soluciones tecnologicas que pueden adquirirse en el mercado, en los procesos y transformaciones de las actividades y procedimientos que aplican las personas, de manera que éstas sean facilitadoras de los mismos, sin sentirse amenazados , sino potenciados por las herramientas que se incorporan.

Es relevante, considerar algunos preceptos claves para ello:

*Instalar la disciplina desde los orígenes de los proyectos que involucran cambios

*Instalar en la ADP[46] como requisito la competencia adaptativa

*Gestionar en las instituciones, empresas, organismos y ciudadanía la adquisición de competencias adaptativas para proyectos de cambio

*Instalar la experiencia usuaria como higiénica en cada proyecto de cambio

Planificar un conjunto de fases que permitan dimensionar y definir las intervenciones que sean requeridas antes, durante y después de concluidos los proyectos que involucran cambios:

[46] ADP: Alta Dirección Pública

Detección de la necesidad del cambio

Tanto factores internos como externos provocan necesidades de cambio, los que son detectados y analizados por el equipo de gestión de cambio, generando una estrategia que se materializa en proyectos de acompañamiento. Los factores de cambio probables vienen desde variables sociales, normativas, internas a la organización, Tecnológicas (Gobierno Digital), Estratégicas y Políticas.

Análisis inicial (diagnóstico)

Se establece una posición frente a la situación deseada. Se debe detectar e identificar perfiles y situaciones específicas que puedan favorecer o dificultar un proceso de transformación. Se identifica el dónde estamos, los proyectos de cambio y el dónde queremos llegar. Un aspecto importante a tener en cuenta es la Gestión de la Demanda que los proyectos harán sobre la organización y su equipo, en donde se debe tener en cuenta que se demandarán esfuerzos específicos sobre algunos actores de la organización, que normalmente, son las personas que más conocen y las que menos tiempo tienen y que deberán dedicar algunas horas de su jornada al proyecto que involucra el cambio.

Implicados y Roles:

Se debe reforzar la importancia del compromiso de todos los actores, especialmente de quienes dirigen el proceso de cambio y su grado de impacto en el éxito o fracaso del cambio organizacional. Se pueden mencionar características positivas/negativas de liderazgo identificar dos conjuntos de actores implicados:

*Red de líderes que están directamente involucrados en el proyecto: directores, subdirectores y mandos medios relacionados con las iniciativas de cambio. Identificar colaboradores que sea necesario involucrar en el liderazgo del proceso de cambio. Establecer metas individuales, objetivos específicos y recompensas.

*Mapa de Implicados: generado por el área de Procesos para identificar colaboradores que será necesario involucrar jerarquizados de acuerdo con el grado de impacto que su participación podrá tener en el proceso.

Planificación:

Se identifica un plan para cada Pilar de Gestión del Cambio:

*Plan de Comunicación y Difusión: Planes diseñados para cada proyecto en particular que la organización esté llevando a cabo y que involucre cambio en acciones, roles, perfiles de las personas. Aseguran el correcto entendimiento de los proyectos por parte de los colaboradores. Contribuyen en el alineamiento de la organización con las iniciativas de cambio. Mantienen oportunamente informada a toda la organización. Contribuye y refuerza el proceso de aprendizaje de los implicados. Las componentes de este plan consideran al menos:

*Objetivos Comunicacionales
*Segmentación
*Medios (Revista; Flash; Cascadas; Reuniones; Convenciones; Intranet)
*Mensajes
* Periodicidad
*Monitoreo y Control
*Feedback

→**Plan de Formación**: contempla la planificación, implementación y control de las iniciativas de formación y entrenamiento. El plan debe responder a identificar las necesidades de formación del equipo que se verá impactado por el cambio en términos de programas de entrenamiento que aborde tanto los aspectos de nuevos procesos, nuevas herramientas, nuevos roles (debe entregar tanto las competencias técnicas como adaptativas). Las componentes de este plan consideran al menos:

*Unidades Involucradas: Identificación – Coordinación – Comunicación – Apoyo
*Personas: Identificación – Convocatoria – Control – Seguimiento
*Cursos: Definición – Validación – Armado – Control – Seguimiento - Datos
*Tiempo: Periodos de capacitación – Fechas claves - Calendarización
*Aspectos Técnicos: Salas – HW y SW – Presentaciones – Manuales de Usuario

→**Plan de Contención y Seguimiento**, El plan debe cubrir, a partir de la identificación de las necesidades de Contención del equipo que requiere ser abordado por la divergencia que generar con respecto al proyecto de cambio, para que, con acciones concretas de mentoring, coaching o acopañamiento de pares, alinearles para que se integren al proceso de cambio y sean un aporte en el mismo y en su implemehtación. Contempla al menos las siguientes acciones:

***Seguimiento Proactivo:**

*Plan de Formación: Evaluación de la experiencia, evaluación del aprendizaje.
*Plan Comunicacional: Evaluación de los medios y la penetración de los mensajes.
*Liderazgo: Seguimiento de la participación de los líderes de la organización

***Seguimiento Reactivo:** análisis y segmentación de incidencias o situaciones reportadas por los colaboradores

***Seguimiento de Maduración:**

*Del nivel de asimilación: Evaluación del grado de aplicación de los procesos y nuevos conocimientos
*Del nivel de productividad: Cuánto ha mejorado el trabajo debido a los nuevos conocimientos y habilidades.

***Coaching, Reprogramación y Recapacitación**

9- DESAFÍOS FUTUROS

9.1 Criterios Tecnológicos:

En cuanto a los criterios de evaluación, diseño, selección e implementación de mecanismos tecnológicos que den cuenta de las definiciones y los planes de trabajo antes mencionados, estos deberán considerar:

*Mantener el principio de neutralidad tecnológica en el Estado, en el sentido de que tanto para el diseño como para la implementación de las soluciones tecnológicas subyacentes, no se privilegien marcas o tecnologías de proveedores específicos de una solución genérica, tendiendo a preferir a seleccionar tecnologías de público acceso, basadas en estándares abiertos y que cuenten con diversos proveedores que permitan apoyar su implementación.

*Sin perjuicio de lo anterior, se deberá tomar a debida consideración los alcances de dependencia que puede implicar una decisión tecnológica y su impacto en la seguridad nacional.

*Privilegiar modelos de soluciones tecnológicas que permitan a la industria nacional adquirir nuevos conocimientos, desarrollar capacidades propias y ventajas comparativas, fortaleciendo la capacidad competitiva de Chile en un contexto global.

*Establecer mecanismos formales y regulares de revisión de las decisiones y diseños establecidos en las normas que sean definidas para estos temas, contrastando las definiciones con el estado del arte del desarrollo tecnológico. Para ello, se establecerán revisiones periódicas y formales (máximo cada 18 meses), que permitan verificar que las decisiones y criterios tecnológicos tomados, permanecen vigentes y acordes al desarrollo de la industria local y mundial.

*Contemplar que los estándares o definiciones tecnológicas incluidas en los diseños, estén acordes con las capacidades técnicas y humanas de Chile para incorporar dichas tecnologías, verificando la capacidad de absorción tecnológica por parte de los agentes contemplados en cada ecosistema.

9.2 Interoperabilidad

Mejorar la eficiencia del Estado simplificando su respuesta a la población, y respondiendo a los requerimientos de esta, son posibles de obtener implementando la Interoperabilidad.

En resumen, es una poderosa herramienta de gestión que permite poner al ciudadano en el centro, promoviendo así las mejores prácticas y normativas para el desarrollo de tecnologías y habilitadores tecnológicos. Implementar la Interoperabilidad importa una decisión política, que por lo demas se respalda en la ley de Modernización del Estado,[47] y los calendarios asociados para su cumplimiento.

[47] Tercera consulta pública Ley N° 21.180, de Transformación Digital del Estado. Norma Técnica de Interoperabilidad. 2021. Gobierno Digital. Gobierno de Chile. Disponible en: https://digital.gob.cl/biblioteca/regulacion/tercera-consulta-publica-ley-n-21180-de-transformacion-digital-del-estado-norma-tecnica-de-interoperabilidad/

Existen múltiples intentos de Interoperabilidad en nuestro país, pero que obedecen a modelos de desarrollo propio, y una importante dispersión de sistemas, politicas y leyes que dificultan la interoperabilidad. Se debe tender a un modelo universal, el cual debe ser adoptado con el convencimiento de ser la mejor solución en las dimensiones, tecnicas, de seguridad y de gestión del cambio. (Ver: experiencia en Uruguay[48] y Colombia,[49] desafíos en Argentina,[50] recomendaciones de Cepal , y X-Road, Interoperabilidad en los países nórdicos).[51]

Acciones a Corto Plazo

*Identificar instancias existentes en donde las clasificaciones de Gobernanza propuestas se puedan ajustar y operar durante un período de transición, instalando en la agenda específica de la instancia las temáticas de la gobernanza y articularlas entre ellas con objetivos y acciones concretas, con la intencionalidad de generar la práctica y la cultura requerida, en el intertanto se cuenta con las capacidades permanentes instaladas.

*Promover una Ley de Interoperabilidad Nacional, que genere las herrramientas administrativas y los recursos para impulsar un modelo de Interoperabilidad para el Estado de Chile, que considere una arquitectura de Interoperabilidad basada en estándares que hayan sido comprobadamente utilizados internacionalmente, y considerando aspectos de politica exterior a objeto de facilitar la interoperabilidad transfronteriza. Dicha ley regulará los aspectos administrativos relativos al intercambio de información entre las instituciones del Estado de manera digital y en tiempo real, con apego estricto a las leyes de Protección de Datos y de Ciberseguridad.

*Creación de la Agencia Nacional de Interoperabilidad, dependiente del Ministerio del Interior, que articule la Interoperabilidad, asuminedo la gobernanza necesaria para administrar los procesos de cambio, y la generación de normas y reglamentos.

*Establecer un proceso de difusión de los procesos de cambio a enfrentar por la Interoperabilidad, y el replanteo de los procesos de gestión interna de las instituciones.

*Establecer un calendario de adopción de la interoperabilidad alineado con lo que establece la ley de Modernización del Estado.

*Promover el estandar de interoperabilidad para su aplicación tanto en el sector público como en el privado. Incentivar el desarrollo de API (Aplication Interfaces) como desarrollos privados.

[48] "Qué es la Plataforma de Interoperabilidad" disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/que-es-la-plataforma-de-interoperabilidad

[49] "Marco de interoperabilidad para Gobierno Digital. Agosto de 2019", Gobierno de Colombia. Disponible en https://www.mintic.gov.co/arquitecturati/630/articles-9375_recurso_4.pdf

[50] "Interoperabilidad en Gestión Pública" tesis Claudia Sánchez, maestría en gestión de servicios tecnológicos y telecomunicaciones, Universidad de San Andrés, Argentina, 2018. Disponible en https://repositorio.udesa.edu.ar/jspui/bitstream/10908/16162/1/%5BP%5D%5BW%5D%20T.%20M.%20Ges.%20S%C3%A1nchez%2C%20Claudia.pdf

[51] "Desde el gobierno digital hacia un gobierno inteligente", Biblioguías, Biblioteca CEPAL. Disponible en https://biblioguias.cepal.org/gobierno-digital/interoperabilidad "Nordic Institute for Interoperability Solutions - NIIS. Disponible en: https://www.niis.org/

Acciones a mediano Plazo y Largo Plazo:

*Administrar el sistema de Interoperabilidad del Estado, adapatandolse a los nuevos requerimientos que surjan de los cambios tecnologicos y los crecientes volumens de información interoperados.

9.3 Identidad Digital

Considerando que se pueden encontrar los siguientes beneficios asociados con el establecimiento de la identidad digital:[52]

*Los derivados directamente de la digitalización de procesos existentes que antes se ofrecían sólo en forma presencial (por ejemplo, la verificación de identidad), y

*Los asociados al surgimiento de nuevos servicios y actividades económicas como resultado del uso de la identidad digital.

Para avanzar en materia de identificación digital y servicios de confianza para las transacciones electrónicas que se realicen tanto en el mercado chileno como internacional, permitiendo otorgar certeza jurídica a infinidad de transacciones entre particulares, empresas y el Estado; desde una perspectiva regulatoria, se deberá robustecer los sistemas vigentes que permitan no solo identificar electrónicamente, sino también autenticar la identidad mediante dos factores, de forma que quien interactúe digitalmente sea realmente sea quien dice ser.

Acciones a Corto Plazo

*Potenciar los mecanismos de autenticación públicos vigentes: ClaveÚnica y Clave Tributaria.

*Establecer una legislación de identidad digital robusta, que radique en el Servicio de Registro Civil e Identificación la emisión y gestión de la identidad digital en Chile. Dicha legislación debe incluir el "domicilio digital" de cada ciudadano, donde se radicará la comunicación entre el Estado y cada ciudadano en particular.

*Incluir en dicha legislación las normas de aplicación claras para el uso de la Identidad Digital por parte de los privados, en concordancia con la Ley de Protección de Datos, actualmente en tramite legislativo, así como la Ley N°21.180 sobre Modernización del Estado.

*Dicha legislación debe considerar aspectos tales como la dependencia técnologica de proveedores y los intereses nacionales, que pudieran verse comprometidos en decisiones de implementación.

[52] "Identidad digital como habilitante estratégico de la transformación digital del país", 2019, OCDE. Gobierno de Chile. Disponible en https: //digital.gob.cl/biblioteca/estudios/identidad-digital-como-habilitante-estrategico-de-la-transformacion-digital-del-pais/

*Para la firma electrónica avanzada, se propone la construcción de un catastro nacional de trámites y procesos para las diversas industrias, que permita la interacción entre agentes públicos y/o privados, recomiende y regule la utilización gradual y progresiva de mecanismos de firma digital, partiendo desde la incorporación de firma digital intermedia hacia firma digital avanzada, dependiendo de la cobertura requerida, realidad tecnológica, complejidad, disponibilidad y estado del arte de los procesos involucrados.

Acciones a Mediano y Largo Plazo

*Promover un mecanismo de identificación y autenticación compatible a nivel latinoamericano, tal como ha venido avanzando Europa a través del Reglamento eIDAS . Este cambio tendría como prerrequisito la regulación de la interoperabilidad, según se ha recomendado en el punto relativo a dicho tema.

*Capítulo 8_*

El Foro Nacional de Ciberseguridad

PARTICIPARON EN LA ELABORACIÓN DE ESTE TEXTO:

- Senador Kenneth Pugh, Michael Heavey, Carolina Muñoz, Julio Cámara, Raimundo Roberts y Tania Yovanovic.

INTRODUCCIÓN

El ciberespacio es un ecosistema íntegramente creado por el ingenio humano, y que ha tenido una vertiginosa evolución. No es una realidad que replique las leyes del mundo físico, pues en este ambiente se pueden construir reglas de convivencia ante nuevas situaciones y desafíos, así como también frente a peligros que sobrepasan la virtualidad, cuyos potenciales efectos pueden afectar severamente nuestro mundo físico, nuestra forma de vivir, los derechos humanos y por supuesto la democracia y la libertad.

De cómo manejar estos peligros y desafíos surge el concepto de la ciberseguridad, término que engloba la seguridad dentro de este nuevo ecosistema.

El derecho a efectuar un uso seguro y confiable del ciberespacio y el contribuir a construir la confianza digital, es una responsabilidad compartida entre todos los actores públicos y privados y el conjunto de la sociedad.

En este contexto, durante el año 2022, el Senado de Chile a través de la Comisión Desafíos del Futuro, Ciencia, Tecnología e Innovación, convocó a más de 140 profesionales provenientes del mundo académico, proveedores, industria y expertos afines, a conformar una Mesa de Ciberseguridad, con el objeto de analizar y visibilizar aspectos de la Ciberseguridad en nuestro país. La mesa se organizó y trabajó sobre 7 tópicos relevantes durante varios meses, y cuyo resultado se comprende en el documento: **"Ciberseguridad para Chile, un camino a recorrer"**, el que alimenta además las acciones de la Estrategia de transformación digital **"Chile Digital 2035".**

La Ciberseguridad es una de las piedras angulares en los procesos de Transformación Digital, siendo **una responsabilidad compartida**, y se deben impulsar todas aquellas medidas que conduzcan a la necesaria cooperación para la seguridad común.

Para dar respuesta a las dudas y preocupaciones que se asocian a un ambiente digital seguro y articular un entorno de colaboración amplio en nuestro país, la Mesa de Ciberseguridad antes mencionada sugiere crear una entidad denominada **"Foro Nacional de Ciberseguridad"**, que convoque de manera organizada a expertos y expertas a fin de canalizar inquietudes e iniciativas sobre la materia, y que esté radicada en el Senado de Chile.

El rol consultivo del Foro permitirá contar con opiniones expertas para el mejoramiento continuo de la normativa legal y reglamentaria, apoyando la actualización de las políticas y estrategias sobre la materia, siendo un referente para la institucionalidad de ciberseguridad nacional, y un apoyo permanente a la Transformación Digital del País.

En su rol difusor, el Foro promoverá la Ciberseguridad a nivel nacional, apoyando y articulando el desarrollo de actividades de promoción y conocimiento, así como la participación nacional en foros internacionales sobre la materia.
La promoción de la cultura de la ciberseguridad es un proceso necesario, al igual que el apoyo a la I+D+i y la creación de una industria nacional que provea soluciones adecuadas a nuestras necesidades.

Inspira la creación de este Foro, la experiencia de España (**https://foronacionalciberseguridad.es**), cuyo foro cumple un rol importante, siendo parte integrante de la gobernanza de ciberseguridad de dicho país.

OBJETIVOS DEL FORO NACIONAL DE CIBERSEGURIDAD

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

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

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

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

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

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

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

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

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

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

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

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

FORMALIZACIÓN DEL FORO

En los últimos años, se han generado diversas iniciativas sobre Ciberseguridad tanto desde el mundo público como el mundo privado. Sin embargo, es importante reconocer la especial preocupación que ha tenido el Senado de la República en estas materias.

A diferencia del Foro español, que es parte de la arquitectura de Ciberseguridad y que se ampara en una estructura del ejecutivo que convoca la participación público-privada, nuestro país está recién creando su gobernanza de Ciberseguridad y es preciso dar pasos para articular la colaboración, facilitar la legislación y darle un sentido prospectivo a la ciberseguridad, y también a los procesos de transformación digital del Estado.

En materias de ciberseguridad, el Senado ha sido históricamente un impulsor, promotor y articulador de estas materias. En efecto, el mes de la ciberseguridad tuvo su origen en moción parlamentaria presentada en el Senado, que dio paso a la Ley N° 21.113 del año 2018, que declara al mes de octubre de cada año como el mes nacional de la ciberseguridad; desde su creación, esta actividad se ha inaugurado tradicionalmente al inicio de cada octubre con una sesión especial de dicha Corporación, dirigida por su Presidente.

Cabe destacar la experiencia obtenida por la Comisión de Desafíos del Futuro del Senado, que ha tenido una importante capacidad de convocatoria, visibilizando así muchos temas señeros más allá de la política. En ella, se piensa en el Chile del mañana, y se aúnan voluntades en pos del futuro de la nación. Es así como han surgido iniciativas como los derechos neuronales, la investigación espacial, desarrollos de diversas especialidades y sus impactos, y por cierto una herramienta de prospección muy poderosa.

También es importante destacar el papel de la Comisión de Transportes y Telecomunicaciones del Senado, la que, reconociendo la importancia de la transformación digital, ha creado instancias de participación que trascienden al ámbito parlamentario, y que han generado una importante visión de futuro, que se refleja por cierto en el documento Chile Digital 2035.

La Mesa de Ciberseguridad de la Comisión Desafíos del Futuro del Senado ha sido una experiencia notable, que ha convocado a discusiones, a compartir visiones y preocupaciones ajenos al avatar político, en una realidad de cambio que demanda y requiere la atención de los especialistas.

La evolución lógica de la mesa, es el Foro Nacional de Ciberseguridad.

El Senado podría impulsar la formalización de una entidad voluntaria, de carácter público privada que convoque a la academia, la sociedad civil, el Estado y las organizaciones gremiales, entre otras, que representan intereses en la ciberseguridad, para aportar a la sana discusión y difusión de conocimientos que se transformen en un referente nacional en la materia.

CONFORMACIÓN EJECUTIVA DEL FORO

El Foro será convocado por el Presidente del Senado, y contará con un Director permanente nombrado por éste, el que se encargará de coordinar y facilitar las actividades de participación de los miembros, encargándose además de promover las actividades del mismo y representarlo en actividades públicas o privadas.

Tendrá un consejo permanente compuesto por 12 miembros: dos Senadores designados por el presidente de la Corporación; se designarán 4 representantes de instituciones seleccionadas por las Comisiones de Transportes y Telecomunicaciones y de Futuro; 4 serán representantes electos por las instituciones representadas en el foro; un representante de la Agencia Nacional de Ciberseguridad y otro de la Agencia Nacional de Protección de Datos (considerando que ambas entidades aún son materia de trámite legislativo, los cargos quedarán vacantes y solo serán cubiertos una vez constituidas dichas agencias).

DE LA MEMBRESÍA DEL FORO

El Presidente del Senado, en su calidad de Presidente del Foro, realizará una invitación amplia a la academia, la sociedad civil, las organizaciones gremiales, las organizaciones no gubernamentales, los colegios profesionales, y las personas afines al ámbito de la ciberseguridad.

Las instituciones serán convocadas para tener representantes permanentes en el Foro, deberán inscribirlos con la respectiva formalidad, y no podrán superar los 5 representantes, de preferencia provenientes de áreas diversas de cada institución. En efecto, considerando que la Ciberseguridad debe abordarse con un criterio multidisciplinario y preferentemente holístico, es importante contar con la participación de distintas sensibilidades que se encuentren involucradas o se vean afectadas por la ciberseguridad.

Se establecerá un reglamento de participación y compromiso de los integrantes del Foro, considerándose la posibilidad de reconocerse la membresía para efectos de promoción personal o institucional, en caso de participación permanente. Esta condición será evaluada según su participación en forma trimestral.

La participación en el foro es a título gratuito; sin perjuicio de lo anterior, y asumiendo la importancia del compromiso asumido por las instituciones participantes, los integrantes nominados se comprometen a apoyar con su tiempo y conocimiento las actividades, sin que ello signifique una dedicación de exclusividad, de forma similar como se participa en actividades gremiales o afines.

Los miembros del Foro se agruparán en mesas de trabajo según afinidad en los temas a tratar, en base a los intereses que manifiesten al inscribirse. Las instituciones podrán hacerlo en más de una mesa, pero solo con un representante por mes

El Foro, excluye la representación individual de empresas de bienes y servicios que comercialicen o promuevan soluciones en Ciberseguridad, servicios digitales de cualquier tipo, comunicaciones, almacenamiento de datos, proveedores de equipos, motores de búsqueda, y otros relacionados o afines, con el objeto de mantener la necesaria transparencia y neutralidad técnica en los análisis y recomendaciones que el Foro realice.

La participación en el Foro es a título gratuito; sin perjuicio de lo anterior, y considerando la importancia del compromiso asumido por las instituciones participantes, los integrantes nominados se comprometen a apoyar con su tiempo y conocimiento las actividades, sin que ello signifique una dedicación de exclusividad, de forma similar como se participa en actividades gremiales o afines.

Los miembros del Foro se agruparán en mesas de trabajo según afinidad en las materias a tratar, en base a los intereses que manifiesten al inscribirse. Las instituciones podrán hacerlo en más de una mesa, pero solo con un representante por mesa.

DE LAS MESAS DE TRABAJO

Una vez constituido el Consejo Permanente, se propondrán las mesas de trabajo según afinidad, pero siguiendo el modelo español y nuestra propia Política Nacional de Ciberseguridad vigente. Se proponen inicialmente las siguientes:

1) ***Cultura de la ciberseguridad.*** Buscando:

***Promover** la difusión de la **cultura de la ciberseguridad como una buena práctica empresarial** y reconocer la implicación de las empresas en la mejora de la ciberseguridad colectiva como responsabilidad social empresarial.

***Concienciar a directivos de organizaciones** a los efectos de que habiliten los recursos necesarios y promuevan los proyectos de ciberseguridad que sus entidades puedan necesitar.

***Promover la concienciación y formación en ciberseguridad** a nivel educacional.

*Promover un **espíritu crítico en favor de una información veraz y de calidad** y que contribuya a la identificación de las noticias falsas y la desinformación.

*Buscar y reconocer la **colaboración y participación de medios de comunicación** para promover la ciberseguridad.

***Apoyar y promover** asociaciones de instituciones agrupadas en temas de ciberseguridad con sus pares internacionales.

2) *Promoción de la industria y a la I+D+i en Ciberseguridad.*
Buscando:

*Estimular el **incremento de la oferta y demanda de productos y servicios de ciberseguridad** de la industria nacional y su internacionalización.

*Generar y promover y articular ecosistemas **de emprendimiento en ciberseguridad**, y en I+D+i en un marco de colaboración público privada

*Impulsar la adopción de medidas de **mejora de la ciberseguridad en Pymes y MiPymes.**

***Estimular** el desarrollo de la industria de ciberdefensa en coordinación con las instituciones de la Defensa Nacional.

3) *Talento y formación en Ciberseguridad.* Buscando:

*Identificar las necesidades de capacidades profesionales de ciberseguridad, fomentando la colaboración con las instituciones educativas y formativas impulsando la formación continua, la **formación para el empleo y universitaria, promoviendo sistemas de acreditación y certificación profesional.**

***Impulsar** la inclusión de **perfiles profesionales de ciberseguridad** en las instituciones del Estado.

***Detectar, fomentar y retener, el talento de ciberseguridad**, mediante programas y actividades coordinadas con la academia.

4) *Marco Regulatorio en Ciberseguridad*

***Proporcionar** elementos de análisis y propuestas en materias de regulación y estratégicas.

***Sistematizar la colaboración** público-privada en las iniciativas de gran impacto transversal o sectorial durante todas las fases del proceso legislativo.

***Contribuir** al conocimiento situacional de las principales tendencias, objetivos y líneas de actuación regulatoria nacionales e internacionales.

***Contribuir** a la evaluación, simplificación, armonización y alineamiento de la normativa vigente.

5) *Transformación Digital*

***Identificar** los principales desafíos que tiene la gestión del Cambio en la Transformación Digital del Estado y su relación con los ciudadanos, y proponer caminos de acción para facilitar su resolución.

***Promover** la búsqueda de soluciones tanto conceptuales como prácticas a problemas que impliquen la gestión del cambio hacia una sociedad digital

***Contribuir** a promover los cambios de la sociedad hacia un uso simple y seguro de la tecnología de la información en la relación del ciudadano con el Estado.

***Apoyar** el desarrollo de la Interoperabilidad en Chile, como mecanismo de mejora permanente de la relación del ciudadano con el Estado.

6) *Tecnologías disruptivas*

***Identificar** las tecnologías disruptivas en el ciberespacio.

***Prospectar** los efectos, positivos y negativos, que puedan tener las tecnologías identificadas, así como su impacto en el ecosistema digital y en otras áreas del país.

***Proponer** medidas de control y mitigación por los efectos adversos y riesgos que puedan importar a la seguridad de las personas, los derechos humanos y la democracia.

***Contribuir** a la difusión de los riesgos y beneficios del uso de herramientas que se deriven de estas tecnologías

7) *Desinformación en línea*

***Identificar** las técnicas utilizadas para promover la diseminación de informaciones falsas, e informaciones imprecisas (Disinformation, misinformation), Deep Fake, funas digitales, sextorsión, phishing, ciberbulling y similares.

***Prospectar** los efectos y formas de influencias de los mecanismos de desinformación, de generación de generación de campañas de desinformación y de manipulación de información en procesos claves para la Democracia, el Estado de Derecho y la libertad de expresión.

***Proponer** estrategias de control, mitigación y puesta en evidencia para contrarrestar efectos contrarios a la seguridad de las personas y sus relaciones interpersonales, del Estado de Derecho y la Democracia.

***Contribuir**, con base a la experiencia internacional, a proponer alternativas para enfrentar estos hechos, desarrollar normativas de control y fiscalización sin afectar los derechos humanos y el Estado de Derecho, pilares de la democracia.

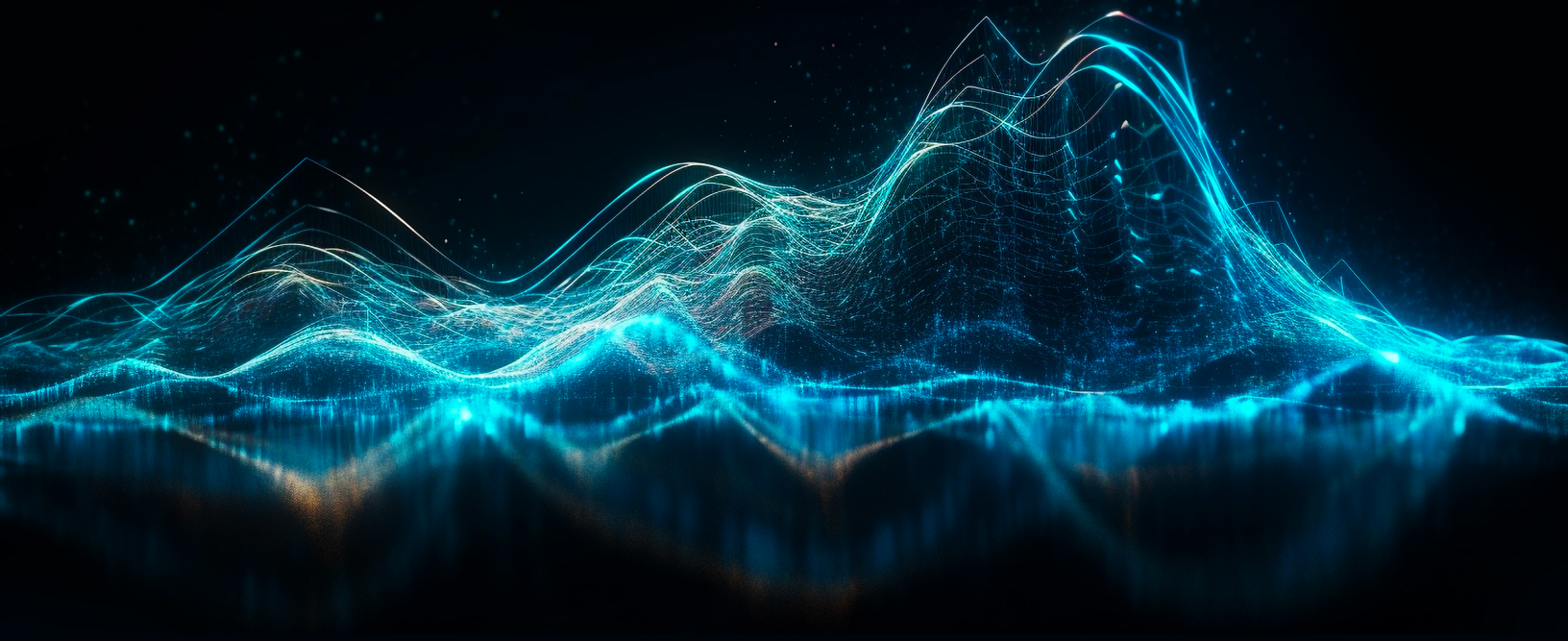
Otras mesas se constituirán en caso de necesidades más específicas, de acuerdo al Consejo Permanente.

FUNCIONAMIENTO DE LAS MESAS DE TRABAJO

Las mesas de trabajo se constituirán inicialmente dirigidas por un equipo de Director/a-Vicedirector/a quienes tendrán la función de coordinar las actividades. Inicialmente serán designados por el Consejo Permanente, para que después sean ratificados o reemplazados por las mayorías absolutas de cada mesa.

Las mesas trabajarán sobre materias específicas que se les soliciten, o atendiendo iniciativas propias que se consideren relevantes y sobre las cuales es importante formar opinión, generando documentos y conclusiones que representen sus posturas, conforme a las reglas que estas mismas se fijen para su funcionamiento, y conforme a formatos estandarizados que se convendrán con el Consejo Permanente.

→CONSTRUYENDO LA CIBERSEGURIDAD EN CHILE←



→COMISIÓN DESAFÍOS DEL FUTURO, CIENCIA, TECNOLOGÍA E INNOVACIÓN←

Biblioteca del Congreso Nacional de Chile / BCN