Ministerio del Interior y Seguridad Pública

Gobierno de Chile

INFORME DE IMPLEMENTACIÓN

POLÍTICA NACIONAL DE CIBERSEGURIDAD

2017-2022



CICS Comité Interministerial sobre Ciberseguridad

Sistema Nacional de CIBERSEGURIDAD

TABLA DE CONTENIDOS

1. INTRODUCCIÓN 02

2. FORMA DE EVALUACIÓN 03
2.1. MEDIDAS Y RESPONSABLES 03
2.2. ESTADO DE LAS MEDIDAS 07

3. CUMPLIMIENTO POR OBJETIVO 08
3.1. INFRAESTRUCTURA RESILIENTE 08
3.2. DERECHOS EN CIBERESPACIO 12
3.3. CULTURA DE CIBERSEGURIDAD 15
3.4. COOPERACIÓN INTERNACIONAL 19
3.5. PROMOCIÓN DE INDUSTRIA 22

4. EVALUACIÓN DE LAS MEDIDAS 24
AVANCE DE LAS MEDIDAS 24
ASPECTOS TRANSVERSALES 28



1. INTRODUCCIÓN

El 27 de abril de 2017 la presidenta Bachelet lanzó la primera Política Nacional de Ciberseguridad de Chile (en adelante, PNCS o simplemente "la Política"). La Política contenía los lineamientos políticos para el Estado en materia de ciberseguridad; esto es, una política de Estado y una serie de 41 medidas a ser implementadas en cuatro años, hasta el año 2022, por diversas subsecretarías y servicios públicos. Estas medidas pretendían avanzar en cinco objetivos de política pública:

A. Infraestructura resiliente: Contar 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.

B. Derechos en ciberespacio: Velar por los derechos de las personas en el ciberespacio.

C. Cultura de ciberseguridad: Desarrollar una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.

D. Cooperación internacional: Establecer relaciones de cooperación en ciberseguridad con otros actores y participar activamente en foros y discusiones internacionales.

E. Promoción de industria: Promover el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos.

Como toda política pública, una vez cumplido el período preestablecido para ella, es necesario evaluar qué medidas y proyectos fueron implementados exitosamente, qué problemas hubo, en qué medida la Política Nacional de Ciberseguridad cumplió con los objetivos fijados inicialmente, y qué lecciones se pueden extraer para el futuro. Este documento contiene una evaluación de la Política, desarrollada por la Coordinación Nacional de Ciberseguridad entre noviembre de 2022 y enero de 2023.

Esta evaluación es necesariamente limitada, y no es una visión externa del avance en la implementación de la Política. Sin embargo, puede servir como insumo para una evaluación externa e independiente.

2. FORMA DE EVALUACIÓN

2.1. MEDIDAS Y RESPONSABLES

En la siguiente tabla se muestran cada una de las 41 medidas incluidas en la Política, además de una breve descripción, el objetivo donde fue considerada y la institución responsable de implementar la medida. Es necesario hacer notar que las medidas 31 a la 41 (ambas inclusive) aportan a más de un objetivo; por tanto, en el reporte del progreso por objetivo, estas medidas serán reportadas dos veces.

En el resto del documento, las iniciativas serán identificadas por su número (columna izquierda).

#	MEDIDA	DESCRIPCIÓN	OBJS.	RESPONSABLE
1	**Proyecto de Ley de Ciberseguridad**	Preparar y enviar al Congreso Nacional un proyecto de Ley sobre ciberseguridad, para consolidar institucionalidad y manejo de incidentes de seguridad informática en el país.	A	Ministerio del Interior y Seguridad Pública
2	**Actualización del DS 83**	Actualizar el DS 83 sobre seguridad de la información del Estado, con miras a la adopción de estándares renovados y a un modelo de control de su cumplimiento efectivo.	A	Subsecretaría General de la Presidencia
3	**Ciberseguridad en contratos de concesión de obras públicas**	Añadir una dimensión de ciberseguridad a la preparación y gestión de contratos de concesión de obra pública.	A	Subsecretaría de Obras Públicas
4	**Grupo de trabajo sobre infraestructuras críticas**	Creación de un grupo de trabajo que establezca un marco normativo y de obligaciones para las infraestructuras críticas en Chile, desde un enfoque de gestión de riesgos.	A	Comité Interministerial sobre Ciberseguridad
5	**Norma técnica para software en el Estado**	Creación de una norma técnica para el desarrollo o contratación de software en el Estado, acorde a estándares de desarrollo seguro.	A	Subsecretaría General de la Presidencia
6	**Plataforma de reporte de incidentes de ciberseguridad**	Creación de una plataforma para agregar información sobre incidentes de ciberseguridad.	A	División de Redes y Seguridad Informática
7	**Normas de seguridad para sectores regulados**	Decretar coordinadamente requisitos actualizados de seguridad para sectores económicos regulados.	A	Subsecretaría de Telecomunicaciones
8	**Riesgos para infraestructuras críticas de información**	Identificar un set mínimo de riesgos para las infraestructuras críticas de la información.	A	División de Redes y Seguridad Informática
9	**Matriz de reportes de incidencias en materia de ciberseguridad**	Implementar una matriz estandarizada para reportes de incidencias en materia de ciberseguridad.	A	División de Redes y Seguridad Informática
10	**Respuesta a desastres informáticos en ONEMI**	Incorporar la dimensión de ciberseguridad en el sistema nacional de emergencias.	A	ONEMI

#	MEDIDA	DESCRIPCIÓN	OBJS.	RESPONSABLE
11	**Norma para comunicación segura entre autoridades**	Preparación de normativa que establezca mecanismos seguros de intercambio de información en el Gobierno, entre autoridades de alto nivel y otros funcionarios que manejen información reservada o secreta.	A	Agencia Nacional de Inteligencia
12	**Estudio sobre resiliencia de telecomunicaciones en Chile**	Preparación de un estudio sobre la resiliencia de las redes de telecomunicaciones en Chile, proponiendo medidas para mejorar la misma en el ámbito público y privado.	A	Subsecretaría de Telecomunicaciones
13	**Actualización Ley de Delito Informático**	Actualizar normativa sobre delitos informáticos.	B	Ministerio del Interior y Seguridad Pública
14	**Plataforma de denuncia de ciberdelitos**	Diseñar e implementar una matriz estandarizada de denuncias de ciberdelitos.	B	Policía de Investigaciones de Chile
15	**Fortalecimiento de capacidades de investigación de ciberdelitos**	Promover el fortalecimiento de las capacidades de investigación y análisis forense relacionadas con el ciberdelito.	B	Policía de Investigaciones de Chile
16	**Sitio web de difusión ciudadana sobre ciberseguridad**	Generar primer punto de difusión de información para el ciudadano sobre ciberseguridad, basado en los diferentes canales electrónicos y redes sociales que ofrece internet.	C	División de Redes y Seguridad Informática
17	**Mes de la ciberseguridad**	Instaurar el mes de la ciberseguridad en octubre de cada año, promoviendo y consolidando actividades de sensibilización en todos los niveles. Además, en febrero participar en el día internet segura.	C	División de Redes y Seguridad Informática
18	**Campaña de ciberseguridad**	Diseñar e implementar una campaña de ciberseguridad de carácter masivo y fomentar la implementación de programas de difusión estableciendo alianzas con los privados en campañas de sensibilización, con énfasis en sectores vulnerables y empleando perspectiva de género.	C	Subsecretaría General de Gobierno
19	**Guías de buenas prácticas para ciudadanos y sector público**	Generar guías de buenas prácticas para la ciudadanía y el sector público.	C	Comité Interministerial sobre Ciberseguridad
20	**Mesa para formación en ciberseguridad a ciudadanía**	Conformar una mesa intersectorial para fomentar la formación en ciberseguridad en todos los niveles y estamentos del sector educativo.	C	Subsecretaría de Educación
21	**Campaña de ciberseguridad para adulto mayor**	Diseñar e implementar una campaña de ciberseguridad orientada a los adultos mayores, que considere medidas de capacitación y difusión.	C	Subsecretaría de Servicios Sociales
22	**Iniciativas de ciberseguridad con ENLACES**	Incorporación de Seguridad en Internet en programas específicos de MINEDUC, reforzando la iniciativa ENLACES.	C	Subsecretaría de Educación

#	MEDIDA	DESCRIPCIÓN	OBJS.	RESPONSABLE
23	**Apoyo a relaciones internacionales**	Apoyar decididamente el establecimiento a nivel internacional de procesos de consultas políticas regionales, subregionales y multilaterales, con especial énfasis en la región.	**D**	Subsecretaría de Relaciones Exteriores
24	**Plan de trabajo para mecanismos bilaterales**	Avanzar en el establecimiento de mecanismos bilaterales de trabajo, diseñando agendas e implementando instancias de consultas políticas transversales con países afines.	**D**	Subsecretaría de Relaciones Exteriores
25	**Política internacional chilena sobre ciberespacio y ciberseguridad**	Elaborar un documento de política internacional de Chile sobre el ciberespacio y ciberseguridad.	**D**	Subsecretaría de Relaciones Exteriores
26	**Grupo interagencial en ciberseguridad**	Establecimiento de un grupo de trabajo interagencial para abordar temas internacionales relativos al ciberespacio.	**D**	Subsecretaría de Relaciones Exteriores
27	**Intercambio de experiencias con otros países en ciberseguridad**	Propiciar el intercambio de experiencias con otros países en materia de ciberseguridad, con énfasis en la implementación y evaluación de estrategias y políticas.	**D**	Subsecretaría de Relaciones Exteriores
28	**Informe sobre regulación de compras públicas**	Analizar la regulación y aplicación del régimen vigente de compras públicas respecto a apoyo productivo e intereses nacionales estratégicos.	**E**	Subsecretaría de Hacienda
29	**Estudios de industria nacional de ciberseguridad**	Realizar estudios tanto de caracterización de la industria de ciberseguridad (oferta), como de acceso y uso de ciberseguridad en el país (demanda), con el objeto de orientar programas especiales para impulsar la industria de ciberseguridad nacional, en sectores definidos.	**E**	CORFO
30	**Estudio de incentivos para estándares de ciberseguridad**	Estudio de incentivos tributarios, subsidios o mecanismos de I+D+i para desarrollo y adopción de estándares de ciberseguridad.	**E**	Subsecretaría de Hacienda
31	**Nueva ley de datos personales**	Tramitar nueva ley de datos personales, con facultades a un órgano específico que pueda imponer requisitos de seguridad y de notificación de filtraciones de datos.	**A,B**	Subsecretaría de Hacienda
32	**Colaboración intersectorial**	Establecer una o más instancias de colaboración multisectoriales con diversos actores sociales (ONG, empresas, gremios, academia y otras).	**A,B,C**	Comité Interministerial sobre Ciberseguridad
33	**Modificación de decretos Red de Conectividad del Estado**	Actualizar DTO 5996 y DS 1299 en coherencia con modificación del DS 83, estableciendo requisitos para acceder a la red (autoevaluación, curso online) y la obligación de reportar incidentes por parte de organismos públicos.	**A,C**	División de Redes y Seguridad Informática

#	MEDIDA	DESCRIPCIÓN	OBJS.	RESPONSABLE
34	**Ciberejercicios con comunidades interesadas**	Realizar ciberejercicios sobre incidentes de ciberseguridad con diferentes comunidades interesadas para fomentar el conocimiento, investigación y difusión adecuada de brechas, vulnerabilidades y vías de mitigación encontradas en los sistemas nacionales.	**A,C**	División de Redes y Seguridad Informática
35	**Estándares de ciberseguridad para proveedores del Estado**	Incorporar estándares de ciberseguridad a los proveedores del Estado, exigiendo requisitos específicos para proveedores TIC, y analizando otros para el resto de los proveedores.	**A,E**	Subsecretaría de Hacienda
36	**Encuesta Nacional Urbana de Seguridad Ciudadana**	Incorporar en la Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC) un set de preguntas vinculadas a los ciberdelitos.	**B,C**	Subsecretaría de Prevención del Delito
37	**Catastro de oferta de capacitación en ciberseguridad para funcionarios públicos**	Generar, y actualizar regularmente, catastro de oferta en capacitación para funcionarios públicos, sobre ciberseguridad disponible en organismos internacionales e instituciones nacionales.	**B,C,D**	División de Redes y Seguridad Informática
38	**Acuerdo de Budapest**	Adherir e implementar la Convención sobre Ciberdelitos del Consejo de Europa.	**B,C**	Ministerio del Interior y Seguridad Pública
39	**Patrocinio de proyectos de I+D en ciberseguridad**	Fomentar el patrocinio del Estado a proyectos de I+D+i con financiamiento público o privado, nacional o internacional en materias de Ciberseguridad.	**C,E**	Comité Interministerial sobre Ciberseguridad
40	**Mesa formación capital humano avanzado en ciberseguridad**	Promover el desarrollo de capital humano avanzado en asuntos de ciberseguridad en los distintos ámbitos técnico-profesionales.	**C,E**	CORFO
41	**Apoyar exportación de productos y servicios de ciberseguridad**	Apoyar la exportación de productos y servicios nacionales en el área de ciberseguridad, identificando ferias internacionales y evaluando posibilidades de apoyo.	**D,E**	Subsecretaría de Relaciones Exteriores

2.2. ESTADO DE LAS MEDIDAS

El resto del documento está organizado en cinco secciones, una por cada objetivo de la Política. En cada sección se describe el avance en el objetivo abordado, junto con la lista de medidas, una breve descripción relativa al contenido de cada una, y en qué estado de cumplimiento se encuentra al momento de escribir este documento. Los estados posibles para una medida son:

- **Cumplida:** La medida fue cumplida completamente, u otra medida con el mismo efecto fue desarrollada en su lugar.
- **Parcialmente cumplida:** La medida fue cumplida parcialmente, u otra medida con el mismo efecto; y no existen esfuerzos actuales por completarla, ya sea porque no existe el presupuesto o la disponibilidad para ello.
- **En proceso:** El servicio responsable informó un cumplimiento parcial, y a la fecha de este informe, está todavía desarrollando actividades.
- **No cumplida:** El servicio responsable informó que no pudo cumplir la medida, y que no se encuentra realizando ningún esfuerzo por completarla actualmente.
- **Sin información:** El servicio responsable fue consultado por las medidas que le fueron asignadas, y a la fecha de este informe todavía no ha respondido.

3. CUMPLIMIENTO POR OBJETIVO

3.1. INFRAESTRUCTURA RESILIENTE

En la siguiente tabla aparece el detalle de cada una de las medidas y su avance dentro de este objetivo:

#	MEDIDA	ESTADO	DESCRIPCIÓN DEL CUMPLIMIENTO
1	**Proyecto de Ley de Ciberseguridad**	**Cumplida**	Se cumple con el proyecto de ley boletín 14847-06. Se preparó y envió al Congreso Nacional el "Proyecto de Ley Marco sobre Ciberseguridad e Infraestructura crítica de la Información" el cual fue aprobado por unanimidad por el Senado, y actualmente se encuentra en el segundo trámite constitucional en la Cámara de Diputados.
2	**Actualización del DS 83**	**En proceso**	En el año 2020 se realizaron varias iteraciones para su modificación, por parte de la División de Gobierno Digital (DGD), existiendo una propuesta final de Decreto que data del mes de febrero del mismo año, pero que no tuvo avances posteriores. No obstante, en el mes de octubre de este año, la División de Gobierno Digital comenzó la reactivación del proceso de modernización de los Decretos Supremos N°s 83 de 2004; 93 de 2006 y 1 de 2015, en conjunto con el CSIRT de gobierno.
3	**Ciberseguridad en contratos de concesión de obras públicas**	**Cumplida parcialmente**	Por contrato las sociedades concesionarias son responsables de la continuidad, actualización, seguridad y confiabilidad de los sistemas de información, sin instrucción explícita sobre prácticas o estándares en materia de ciberseguridad. A futuro, la División de Gestión de Contratos estudiará a través de una asesoría la integración en las bases de licitación de los próximos contratos que se oferten, mayores obligaciones específicas para las sociedades concesionarias en materia de ciberseguridad.
4	**Grupo de trabajo sobre infraestructuras críticas**	**No cumplida**	No se presentan avances de implementación.
5	**Norma técnica para software en el Estado**	**Cumplida**	Se cuenta con la guía técnica de "Lineamientos para el desarrollo de software", en su segunda versión de mayo de 2021, que contiene un acápite sobre desarrollo seguro y se encuentra disponible en la página web de la División de Gobierno Digital.
6	**Plataforma de reporte de incidentes de ciberseguridad**	**Cumplida**	Se ha implementado una plataforma interna al CSIRT de gobierno, utilizando el software OTRS para agregar incidentes que puedan ser clasificados dentro de la taxonomía de ENISA. Los canales de alimentación son ***www.csirt.gob.cl***, ***soc@interior.gob.cl***, el número telefónico +56 2 24863850 y el número corto de emergencia 1510.
7	**Normas de seguridad para sectores regulados**	**Cumplida parcialmente**	Mediante Resolución exenta N° 1.318 de 2020, se aprobó la Norma Técnica sobre Fundamentos Generales de ciberseguridad para el diseño, instalación y operación de redes y sistemas utilizados para la prestación de servicios de telecomunicaciones, que establece el marco regulatorio que comprenda los fundamentos generales de ciberseguridad en base a los cuales deben ser diseñadas, instaladas y operadas de manera segura las redes y sistemas utilizados para la prestación de servicios de telecomunicaciones regulados por la ley N°18.168, teniendo en consideración el resguardo y la resiliencia de las redes, sistemas y su continuidad operacional, confidencialidad, integridad y disponibilidad de la información.

#	MEDIDA	ESTADO	DESCRIPCIÓN DEL CUMPLIMIENTO
8	Riesgos para infraestructuras críticas de información	**No cumplida**	No se presentan avances de implementación.
9	Matriz de reportes de incidencias en materia de ciberseguridad	**Cumplida**	Se adoptó la taxonomía de ENISA en plataforma MISP (Malware Information Sharing Platform).
10	Respuesta a desastres informáticos en ONEMI	**Cumplida**	Desde el año 2015 ONEMI está implementando controles de la ISO 27001, abarcando distintas dimensiones de control en materia de seguridad de la información y ciberseguridad, como: • Controles lógicos en las plataformas de tecnología • Controles físicos • Controles relacionados al trabajo remoto • Inventario y categorización de los Sistemas Críticos (Sistemas de Alerta de Emergencia, Sistema de Sirenas, Sistemas Satelitales y de Radio comunicación entre otros). Adicionalmente, ONEMI se ciñe a las recomendaciones en materia de ciberseguridad que emite el Equipo CSIRT permanentemente.
11	Norma para comunicación segura entre autoridades	**No cumplida**	Para sugerir una norma de comunicación segura la Agencia Nacional de Inteligencia considera necesario establecer un estándar común en las instituciones del Estado. En materia de telefonía fija existe un sistema IP cifrado para altas autoridades cuya operación está a cargo de Presidencia. En telefonía móvil el tema es más complejo. La experiencia en gobiernos anteriores es que hubo algunos sectores, en especial de la Defensa, que usaban sistemas específicos que no eran compatibles fuera de entornos institucionales. En los últimos años se había avanzado en una mayor estandarización pero el esfuerzo, al no ser normado, no ha sido consistente. Actualmente la Agencia Nacional de Inteligencia se encuentra cerrando la evaluación de la plataforma ELEMENT en cuanto a capacidades y seguridad. Esto permitiría elevar los estándares respecto de otras aplicaciones como Signal o Whatsapp. Cabe señalar que ELEMENT está siendo testeado a través del Subcomité de Ciberseguridad que encabeza la ANI y que involucra tanto a policías como Fuerzas Armadas, por lo que el Sistema de Inteligencia del Estado ha estado comprometido en avanzar en esta materia.
12	Estudio sobre resiliencia de telecomunicaciones en Chile	**Cumplida**	Se desarrolló un estudio elaborado por NIC Chile, Universidad de Chile, Proyecto Innova Chile, CORFO 15BPE-47225: “Estudio y recomendaciones sobre la resiliencia de la infraestructura de la Internet chilena”. Este estudio hace un diagnóstico de la red chilena, proponiendo la forma más eficiente en que el país puede invertir para construir nuevos trazados, avanzando en el entendimiento de la resiliencia (tolerancia a fallas, ataques y catástrofes) de Internet en general aplicándolo a la red chilena en particular. Sobre esta medida, la institución advierte que no disponen de recursos para la revisión del estudio durante el año 2023, existiendo la posibilidad de actualizarlo el año 2024.

#	MEDIDA	ESTADO	DESCRIPCIÓN DEL CUMPLIMIENTO
31	Nueva ley de datos personales	En proceso	El proyecto de ley de datos personales se encuentra en segundo trámite constitucional de la Cámara de Diputados.
32	Colaboración intersectorial	No cumplida	No se presentan avances de implementación.
33	Modificación de decretos Red de Conectividad del Estado	En proceso	Existe un borrador de modificación de los decretos que requieren ser revisados.
34	Ciberejercicios con comunidades interesadas	Cumplida	Se han realizado anualmente ejercicios de simulación a cargo de CSIRT involucrando a los encargados de ciberseguridad y de las Áreas TI.
35	Estándares de ciberseguridad para proveedores del Estado	Cumplida	Para llevar a cabo dicho compromiso, la Dirección de Compras y Contratación Pública ha preparado recomendaciones generales para los compradores públicos, para que sean ellos, a partir de sus respectivos requerimientos de compra, formalizados en las bases de licitación o en el requerimiento de un trato directo, sea quienes exijan el cumplimiento de estándares de ciberseguridad por parte de los oferentes, dentro de la normativa vigente. Se actualizaron los términos y condiciones de uso de la plataforma ***www.mercadopublico.cl*** para establecer las responsabilidades de los proveedores y compradores en el uso de cuentas de acceso, se actualizaron los requerimientos hardware y software (PC, aplicaciones y sistema operativo) para prevenir vulnerabilidaddes, malware y otras amenazas, a través de la Resolución Exenta N° 585-B, de 02 de septiembre del 2021, de la Dirección de Compras y Contratación Pública, la cual "Aprueba nuevas políticas y condiciones de uso del sistema de información de compras públicas y registro de proveedores" ***https://www.chilecompra.cl/wp-content/uploads/2021/09/585-B-Res.-Aprueba-Nuevas-Politicas-y-Condiciones-de-uso.pdf***

En términos generales, hubo avances importantes. La Subsecretaría de Telecomunicaciones y la Universidad de Chile (a través de NIC Chile) realizaron un estudio sobre la resiliencia de Internet en Chile (medida 12); este no sólo es un primer paso para entender qué tan frágil es la infraestructura de redes de nuestro país, sino que es un ejemplo notable de investigación aplicada al avance del país y de sus intereses.

En términos normativos, tenemos nuevas regulaciones, o proyectos de ley muy avanzados en ciberseguridad o en áreas relacionadas, que nos ayudarán a que instituciones de gobierno y entidades privadas cumplan con estándares mínimos de seguridad:

- El Proyecto de Ley Marco de Ciberseguridad se encuentra en una etapa avanzada de discusión legislativa, que establecerá una nueva institucionalidad de ciberseguridad para el país y permitirá fortalecer la infraestructura de Internet (medida 1).
- La Subsecretaría General de la Presidencia generó una guía técnica para el desarrollo seguro de software en el Estado; muchas instituciones hoy desarrollan software, y medidas como ésta ayudan a mejorar los estándares de desarrollo (medida 5).
- La Subsecretaría de Telecomunicaciones aprobó una norma técnica sobre fundamentos generales de ciberseguridad, aplicable a los prestadores de servicios de telecomunicaciones (medida 7).

En relación a avances de control de gestión:

- La Subsecretaría del Interior implementó una plataforma de reporte de incidentes de seguridad (medida 6) y adaptó la taxonomía de ENISA para la recepción de datos de incidentes (medida 9). En conjunto, estas medidas estandarizan la recepción, tratamiento y respuesta a incidentes.
- ONEMI (servicio que en 2023 cambió de nombre a SENAPRED) incorporó controles de seguridad a los procesos que gestionan (medida 10), lo que no sólo aumenta la seguridad de los procesos gestionados sino que genera externalidades positivas sobre el resto de la administración pública. En el caso de la medida 3, la Subsecretaría de Obras Públicas indicó que a pesar de que en las concesiones de obras públicas no se exigen requisitos específicos sobre ciberseguridad, estudiarán la posibilidad de incorporarlos a futuro.

En términos de avance en entrenamiento y concienciación, el CSIRT de gobierno realiza anualmente entrenamientos simulados con otros organismos del sector público para entrenarlos (medida 34).

Hubo también medidas que no fueron concretadas o que se encuentran aún en proceso. Para la mayor parte de estas medidas, se sugerirá que sean reincluidas en la nueva Política Nacional de Ciberseguridad. En el ámbito normativo:

- A pesar de que se realizó un esfuerzo importante no se actualizó el Decreto Supremo 83 de 2004 (medida 2), del Ministerio Secretaría General de la Presidencia, que durante más de 10 años impuso normas sobre seguridad de la información a servicios públicos. Sin embargo, en el corto plazo se propondrán no sólo actualizaciones a ese decreto, sino también a los decretos 93 de 2006 y 1 de 2015, con lo que tendremos mejores normas sobre seguridad de la información para el sector público.
- A la fecha de este informe, la ley de protección de datos personales (medida 31) no ha sido promulgada y su discusión se encuentra en segundo trámite constitucional de la Cámara de Diputados.

En los ámbitos de control de gestión, colaboración intersectorial y otros:

- No se logró generar un canal de comunicación seguro entre autoridades (medida 11).
- No se logró identificar un conjunto mínimo de riesgos para las infraestructuras críticas de información (medida 8).
- No se generaron instancias de colaboración multisectoriales sobre temas de ciberseguridad (medida 32). El objetivo es tener medios a través de los cuales tanto el sector privado, las organizaciones no gubernamentales, la academia y la sociedad civil tenga la posibilidad de exponer sobre problemas en ciberseguridad, e intentar encontrar en conjunto soluciones.
- No se logró generar un grupo de trabajo sobre infraestructura crítica (medida 4).

3.2. DERECHOS EN CIBERESPACIO

En la siguiente tabla aparece el detalle de cada una de las medidas y su avance dentro de este objetivo.

#	MEDIDA	ESTADO	DESCRIPCIÓN DEL CUMPLIMIENTO
13	**Actualización Ley de Delito Informático**	**Cumplida**	Esta medida se cumple con la Ley 21.459, publicada en el Diario Oficial el 20.06.2022 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.
14	**Plataforma de denuncia de ciberdelitos**	**Cumplida parcialmente**	PDI: se trabajó en conjunto con el CSIRT de gobierno en la "Matriz de Clasificación de Incidentes", como una forma de establecer una definición común para todos los actores, especialmente cuando nos vemos enfrentados a un incidente informático que constituyan delitos. Dicha matriz fue publicada en el sitio web ***https://www.csirt.gob.cl/matriz-clasificacion-incidentes/***, sin embargo, se debe contemplar la actualización de dicha matriz de acuerdo a la ley de delitos informáticos actual. Adicionalmente, como una forma de poner en funcionamiento en parte esta medida, se desarrolló la iniciativa denominada "Denuncia Violencia Digital" ***https://www.gob.cl/saludablemente/violenciadigital/denuncia/***; para ello, la PDI dispuso un número telefónico vía WhatpApp para víctimas de situaciones de ciberacoso. Este servicio funciona 24/7 y es atendido por oficiales PDI de cibercrimen, los cuales entregan asesoría y también reciben denuncias de manera telemática cuando corresponde.
		Sin información	Carabineros: No se presentan avances de implementación.

#	MEDIDA	ESTADO	DESCRIPCIÓN DEL CUMPLIMIENTO
15	**Fortalecimiento de capacidades de investigación de ciberdelitos**	**Cumplida**	PDI: la PDI creó en marzo de 2022 la Jefatura Nacional de Cibercrimen (JENACIBER), cuyo objetivo es ser la encargada de dirigir y supervisar a las Brigadas Investigadoras de Cibercrimen, generando las condiciones para una efectiva investigación criminal por parte de las unidades dependientes. Desde el punto de vista estratégico se encuentra sustentada en cuatro pilares: Infraestructura, capital humano, capacitación y tecnología, buscando con ello potenciar el área relacionada a la persecución penal del delito informático. Adicionalmente, desde fines de 2022 se está trabajando en un plan para la generación de capacidades PDI a nivel regional a lo largo del territorio nacional, que contribuya a mejorar la primera respuesta en aquellos delitos comunes potenciados por los medios informáticos. En esa misma línea, bajo el alero de la JENACIBER se procedió a crear el Departamento Forense Digital, como una forma de brindar asesoría y apoyo directo a las Brigadas Investigadoras del Cibercrimen, mejorando con ellos los estándares relativos a imparcialidad y objetividad en el proceso del tratamiento de la evidencia digital, en el contexto de una investigación penal.
		Sin información	Carabineros: No se presentan avances de implementación.
31	**Nueva ley de datos personales**	**En proceso**	Segundo trámite constitucional/ Cámara de Diputados
32	**Colaboración intersectorial**	**No cumplida**	No se presentan avances de implementación.
36	**Encuesta Nacional Urbana de Seguridad Ciudadana**	**Cumplida**	En el marco de mejoras en la aplicación anual de la ENUSC, el año 2014 la entonces Subsecretaría implementó un consejo de expertos que propuso realizar mejoras en la medición y contenido de la encuesta. Entre estas mejoras, se contempló un apartado de consulta de victimización por delitos cibernéticos. Desde el año 2015 al 2021 la ENUSC cuenta con indicadores de delitos cibernéticos descritos para el nivel país, así como a nivel regional. Se encuentran disponibles tanto las bases de datos como los informes de resultados de la encuesta de años 2015 a 2021, en los cuales se reporta el indicador de prevalencia de delitos cibernéticos. Esta información es de acceso público y puede ser descargada de los portales de información de la Subsecretaría[1] y el INE[2]. Para el año 2022, la Subsecretaría, en conjunto con el INE, organismo técnico que implementa la encuesta, se encuentran planificando una actualización en términos de diseño muestral y delitos abordados por el instrumento, teniendo como referencia encuestas de victimización a nivel internacional y propuestas regionales como la VICLAC, que cuenta con apoyo de UNODC.

[1] Ver *http://cead.spd.gov.cl/estudios-y-encuestas/*
[2] Ver *https://www.ine.cl/estadisticas/sociales/seguridad-publica-y-justicia/seguridad-ciudadana*

#	MEDIDA	ESTADO	DESCRIPCIÓN DEL CUMPLIMIENTO
37	Catastro de oferta de capacitación en ciberseguridad para funcionarios públicos	No cumplida	No hay un levantamiento y catastro formal de oferta de capacitación para funcionarios y debidamente publicado en un sitio web accesible por el público objetivo o bien mecanismo de difusión.
38	Acuerdo de Budapest	Cumplida	El 12 de mayo del 2022 nuestro país firmó el segundo protocolo, en el marco de la conferencia internacional sobre cooperación reforzada y divulgación de pruebas electrónicas. El paso siguiente es comenzar el trabajo para la ratificación del Segundo Protocolo, incluyendo las reservas y declaraciones que el Gobierno de Chile estime necesario incluir. Al respecto, tanto el Ministerio del Interior como el Ministerio de Justicia han informado al Ministerio de Relaciones Exteriores sobre sus respectivas propuestas (en particular respecto a los artículos 7 y 8 del texto), a objeto de que sean analizadas por DIGEJUR.

En este ámbito, los avances más importantes fueron la firma del Acuerdo de Budapest (medida 38) y la actualización de la Ley de Delito Informático (medida 13), tanto para modernizar esta última como para armonizar nuestros tipos penales con el Acuerdo de Budapest. Ambas medidas permitirán proteger de mejor forma los derechos de las personas en nuestro país al facilitar la coordinación con organismos internacionales y la compartición de información.

De igual forma es destacable también la inclusión de la ciberseguridad en la Encuesta Nacional Urbana de Seguridad ciudadana (ENUSC), por la Subsecretaría del Delito (medida 36), y el fortalecimiento de las capacidades de investigación de la Policía de Investigaciones (medidas 14 y 15), ya revisadas en el objetivo anterior.

El siguiente es un resumen de la medida que no se concretó en este objetivo: no se generó un catastro de oferta de capacitación para funcionarios públicos en materia de ciberseguridad (medida 37), lo que hubiera contribuido a acelerar la formación y conciencia del tema en los funcionarios públicos. Se sugerirá incluir nuevamente esta medida en la nueva Política Nacional de Ciberseguridad.

3.3. CULTURA DE CIBERSEGURIDAD

En la siguiente tabla aparece el detalle de cada una de las medidas y su avance dentro de este objetivo:

#	MEDIDA	ESTADO	DESCRIPCIÓN DEL CUMPLIMIENTO
16	**Sitio web de difusión ciudadana sobre ciberseguridad**	**Cumplida**	Se han implementado varios canales de difusión articulados por el CSIRT (sitio web y redes sociales) teniendo presente distintos públicos objetivo. Además de participar en campañas públicas y asociaciones con privados.
17	**Mes de la ciberseguridad**	**Cumplida**	Esta es una actividad que se realiza de manera anual.
18	**Campaña de ciberseguridad**	**Cumplida**	El departamento de marketing perteneciente a la División Secretaría de Comunicaciones (SECOM), asesoró al Ministerio del Interior y Seguridad Pública en una campaña sobre la materia durante el 2018, la que contó con minutos otorgados por CNTV para la emisión por los canales de televisión abierta en horario prime. La campaña fue emitida en diciembre 2018 y enero 2019[3]. La campaña lleva más de 3 años sin ser difundida nuevamente.
19	**Guías de buenas prácticas para ciudadanos y sector público**	**Cumplida parcialmente**	Esta guía fue generada y está disponible, pero no se ha hecho difusión de ella.
20	**Mesa para formación en ciberseguridad a ciudadanía**	**Cumplida**	Hasta 2018, en el marco de un convenio con la Unesco, el Ministerio de Educación, a través del Centro de Educación y Tecnología - Enlaces, convocó a instituciones públicas, privadas y de la sociedad civil a integrarse a una Red de Ciudadanía Digital, a fin de generar un espacio de diálogo multidisciplinario para orientar la política pública respecto a la formación en ciudadanía digital de la comunidad educativa. Dicho grupo de trabajo definió, en su primera etapa, entregar lineamientos para el desarrollo de contenidos y materiales educativos que llegaron a la comunidad educativa a través del MINEDUC y los materiales generados fueron publicados en el sitio ***http://www.internetsegura.cl/.*** Sin embargo, a contar de 2018, la autoridad de la época dispuso que estos temas fueron abordados por otra unidad ministerial, la División de Educación General, quedando la mesa de Ciudadanía Digital en manos de otras instituciones, dejando de funcionar. El sitio web no ha sido actualizado desde esa fecha. Durante el año 2022, la temática de ciudadanía digital (relacionada con la medida N°20 de la PNCS) ha vuelto a estar radicada en el Centro de Innovación del Ministerio y se ha conformado una mesa de trabajo multidepartamental. En esta mesa se está abordando la ciberseguridad desde la perspectiva de ciudadanía digital, dentro de una dimensión que se ha definido como "Cuidado y Responsabilidades Digitales". Esta iniciativa tiene entre sus próximos hitos relanzar, durante el primer semestre de 2023, la plataforma web ***http://www.ciudadaniadigital.cl*** donde se pondrá a disposición de la comunidad educativa distintos recursos relacionados con la temática de ciberseguridad.

[3] El spot de la campaña y su plan de medios puede ser encontrado en el siguiente link:
https://www.dropbox.com/sh/riiiue2f5lxio5k/AACBw1pZ3vKTDTuUoXG0K8Dwa?dl=0

#	MEDIDA	ESTADO	DESCRIPCIÓN DEL CUMPLIMIENTO
21	**Campaña de ciberseguridad para adulto mayor**	**Cumplida**	Se desarrollaron las siguientes acciones: **a) Noviembre, 2020:** SENAMA, en conjunto con la Subsecretaría del Interior, lanza campaña educativa sobre conciencia digital para adultos mayores. Ésta busca guiar y apoyar a los adultos mayores para evitar que sean víctimas de algún tipo de estafa cibernética. Consiste en seis cápsulas de videos que abordan la importancia de la privacidad en internet, explicando, por ejemplo, qué es la ciberseguridad, un ciberdelito, phishing, se presentan los tipos de delitos, cómo identificar una estafa y recomendaciones. La campaña se encuentra disponible en las redes sociales y en el sitio web ***www.concienciadigital.gob.cl*** **b) Enero, 2021:** Dirigentes de personas mayores del país se capacitan en ciberseguridad por medio de una charla, organizada por el programa Escuela de Formación para Dirigentes Mayores de SENAMA. "Ciberseguridad y Redes Sociales, ¿cómo estar prevenidos?" fue el nombre de la charla realizada por el oficial de Seguridad de la información de la Universidad de Chile, Andrés Peñailillo, y donde participaron dirigentes mayores, de las 16 regiones del país. Entre los temas abordados destacaron: las redes más utilizadas, recomendaciones de seguridad, como, por ejemplo: para generar contraseñas seguras, además se habló de los distintos tipos de estafas por canales digitales, entre otros temas. **c) Septiembre, 2022:** En el marco del Fondo de Innovación, perteneciente al componente de Convenios Institucionales del Fondo Nacional del Adulto Mayor, se establecieron como temáticas a desarrollar: Salud Mental e Inclusión Digital, en ésta se solicitó a los oferentes que presentaran los proyectos, con especial énfasis en ciberseguridad para personas mayores. Este fondo se encuentra en proceso de revisión de antecedentes y adjudicación.
22	**Iniciativas de ciberseguridad con ENLACES**	**En proceso**	Destacamos que la enseñanza de lo relativo a ciberseguridad estará incorporado en las acciones formativas, recursos pedagógicos y orientaciones que apunten al desarrollo de la ciudadanía digital, toda vez que uno de los ejes estratégicos ministeriales es avanzar hacia una educación integral, inclusiva y que responda a los desafíos de la sociedad en el siglo XXI. En esta misma línea, la Política de Reactivación Educativa Integral "Seamos Comunidad" tiene como uno de sus ejes el "Plan de Transformación digital y conectividad", que considera el desarrollo de las capacidades de las comunidades educativas en todos sus niveles para aprovechar el potencial de las tecnologías digitales de forma crítica, responsable, participativa y creativa. Por otro lado, en el próximo ciclo de reforma curricular, parte de la Política de Desarrollo Curricular que está diseñando la Unidad de Currículum y Evaluación, se espera debatir sobre los ejes basales y transversales de aprendizaje, donde lo relacionado a Ciudadanía Digital (y ciberseguridad como parte de ella) será considerado.
32	**Colaboración intersectorial**	**No cumplida**	No se presentan avances de implementación.
33	**Modificación de decretos Red de Conectividad del Estado**	**En proceso**	Existen borradores de modificación de los decretos que requieren ser revisados.

#	MEDIDA	ESTADO	DESCRIPCIÓN DEL CUMPLIMIENTO
34	Ciberejercicios con comunidades interesadas	Cumplida	Se han realizado anualmente ejercicios de simulación a cargo de CSIRT involucrando a los encargados de ciberseguridad y de las áreas TI.
36	Encuesta Nacional Urbana de Seguridad Ciudadana	Cumplida	En el marco de mejoras en la aplicación anual de la ENUSC, el año 2014 la entonces Subsecretaría implementó un consejo de expertos que propuso realizar mejoras en la medición y contenido de la encuesta. Entre estas mejoras, se contempló un apartado de consulta de victimización por delitos cibernéticos. Desde el año 2015 al 2021 la ENUSC cuenta con indicadores de delitos cibernéticos descritos para el nivel país, así como a nivel regional. Se encuentran disponibles tanto las bases de datos como los informes de resultados de la encuesta de años 2015 a 2021, en los cuales se reporta el indicador de prevalencia de delitos cibernéticos. Esta información es de acceso público y puede ser descargada de los portales de información de la Subsecretaría[4] y el INE[5]. Para el año 2022, la Subsecretaría, en conjunto con el INE, organismo técnico que implementa la encuesta, se encuentran planificando una actualización en términos de diseño muestral y delitos abordados por el instrumento, teniendo como referencia encuestas de victimización a nivel internacional y propuestas regionales como la VICLAC, que cuenta con apoyo de UNODC.
37	Catastro de oferta de capacitación en ciberseguridad para funcionarios públicos	No cumplida	No hay un levantamiento y catastro formal de oferta de capacitación para funcionarios y debidamente publicado en un sitio web accesible por el público objetivo o bien mecanismo de difusión.
39	Patrocinio de proyectos de I+D en ciberseguridad	No cumplida	No se presentaron avances en esta medida. Se enviará oficio al Ministerio de Ciencia preguntando por proyectos de I+D.
40	Mesa formación capital humano avanzado en ciberseguridad	Cumplida	Respecto de la medida N°40, se han desarrollado las siguientes actividades: • 2019 (18pfc-99573): programa de formación para la seguridad de la información y la ciberseguridad, con el objetivo de generar competencias en materia de seguridad de la información y ciberseguridad en trabajadores que se desempeñen laboralmente en pequeñas y medianas empresas (pymes) y cuyo negocio implique un uso intensivo de sistemas digitales de información. • 2022 (22pfc-201213): formación para siete perfiles laborales TIC de especialidad 2022: formar capital humano especializado en los perfiles de data analyst (análisis de datos), *data scientist* (ciencia de datos), arquitectura cloud, especialización devops, especialización IoT, ciberseguridad y *lean-agile business developer*, desarrollando acciones que permitan masificar estas temáticas.

[4] Ver *http://cead.spd.gov.cl/estudios-y-encuestas/.*
[5] Ver *https://www.ine.cl/estadisticas/sociales/seguridad-publica-y-justicia/seguridad-ciudadana.*

En este objetivo también hubo avances importantes. El siguiente es un resumen de lo que se logró en el objetivo de cultura de ciberseguridad:

1. La Subsecretaría del Interior generó un sitio de difusión de información sobre ciberseguridad del CSIRT de gobierno, donde semanalmente se actualizan contenidos para el público general (medida 16); se realizan además diversas actividades de difusión todo el año, pero especialmente durante octubre, mes de la ciberseguridad (medida 17).

2. La Subsecretaría de Educación gestionó instancias de diálogo con la sociedad civil sobre ciberseguridad; y se planifica incluir contenido de ciberseguridad en la próxima reforma curricular como parte de la iniciativa de Ciudadanía Digital (medida 20).

3. La Subsecretaría de Gobierno realizó una campaña de seguridad abierta al público a través de la televisión (medida 18); y la Subsecretaría de Servicios Sociales implementó diversas medidas para capacitar y concienciar al adulto mayor sobre la importancia de la protección de sus datos personales (medida 21).

4. CORFO implementó dos programas de formación (medida 40): uno para trabajadores de PYMEs cuyo negocio implique el uso intensivo de tecnologías de información, y otro para personas con perfiles técnicos más avanzados.

Sin embargo, hubo también medidas importantes en las que no hubo avance. La principal es la medida 39: no se logró diseñar ni implementar un programa de financiamiento de proyectos de investigación y desarrollo (I+D) en ciberseguridad. Esta es una medida central, que nos permitiría definir áreas de financiamiento preferente de proyectos de I+D por parte de ANID y CORFO. Se propondrá el incluir nuevamente esta medida dentro de la nueva Política Nacional de Ciberseguridad.

Finalmente, no se incorporó contenido específico sobre ciberseguridad en los programas específicos de educación básica o media por parte del Ministerio de Educación (medida 22). Sin embargo, en el próximo ciclo de reforma curricular la Unidad de Currículum y Evaluación espera poder debatir sobre los ejes basales y transversales de aprendizaje, donde lo relacionado a Ciudadanía Digital, y ciberseguridad como parte de ella, será considerado.

3.4. COOPERACIÓN INTERNACIONAL

En la siguiente tabla aparece el detalle de cada una de las medidas y su avance dentro de este objetivo:

#	MEDIDA	ESTADO	DESCRIPCIÓN DEL CUMPLIMIENTO
23	Apoyo a relaciones internacionales	Cumplida	En abril del 2017 se aprobó establecer un grupo de trabajo para que elabore un conjunto de medidas de fomento y cooperación y confianza en el ciberespacio, del cual Chile forma parte y ya ha participado en cuatro reuniones sobre esta materia. Desde el 2019 a 2022 Chile participó en todas las reuniones del Grupo de Trabajo de Composición Abierta sobre los avances en la Esfera de la Información y Telecomunicaciones en el Contexto de la Seguridad Internacional (OEWG). En esta misma materia, Francia junto a Egipto propusieron establecer un "Programa de Acción (PoA) sobre comportamiento responsable de los Estados en el ciberespacio", el cual Chile apoya junto a otros siete países de la región. El PoA fue adoptado recientemente en la primera comisión de la Asamblea General (3 de noviembre de 2022). Con fecha 27 de diciembre de 2019 la Asamblea General de Naciones Unidas aprobó el proyecto de resolución presentado por la delegación de Rusia, en nombre de otras siete naciones, en la 44ª sesión del 7 de noviembre. El proyecto se denomina: "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos" (A/RES/74/247). La principal finalidad de este proyecto es: "establecer un comité intergubernamental especial de expertos de composición abierta, representativo de todas las regiones, a fin de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, teniendo plenamente en cuenta los instrumentos internacionales y las iniciativas existentes en los planos nacional, regional e internacional para combatir la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, en particular, la labor y los resultados del grupo de expertos encargado de realizar un estudio exhaustivo sobre el delito cibernético, de carácter intergubernamental y de composición abierta". Hasta la fecha se han realizado tres reuniones del Comité Especial; MINREL ha participado en todas. En los últimos años Chile ha participado en iniciativas internacionales sobre ciberseguridad que buscan promover un ciberespacio abierto, seguro, y estable, como también el comportamiento responsable de los Estados en dicho ámbito.
24	Plan de trabajo para mecanismos bilaterales	Cumplida	Se avanzó en la conformación de Grupos de Trabajo de los MOUs ya firmados, y se fomento la realización de diálogos entre Cancillerías. MOUs firmados: Argentina, Colombia, Ecuador, España, Estonia, Israel, Reino Unido, OEA. En la actualidad existen acuerdos pendientes de firma y/o negociación con los siguientes países: Corea, Singapur, Finlandia, Japón, República Dominicana, Italia, Uruguay, Costa Rica, entre otros. MISP señaló en 2022 que se abocará en una revisión de los textos firmados y otros por firmar.

#	MEDIDA	ESTADO	DESCRIPCIÓN DEL CUMPLIMIENTO
25	Política internacional chilena sobre ciberespacio y ciberseguridad	**No cumplida**	No se ha desarrollado a la fecha un documento específico sobre el particular.
26	Grupo interagencial en ciberseguridad	**No cumplida**	No se ha establecido un grupo específico sobre el particular.
27	Intercambio de experiencias con otros países en ciberseguridad	**Cumplida**	No se han realizado avances específicos, pero es posible incorporar las dinámicas de trabajo y cooperación descritas en la medida 24.
37	Catastro de oferta de capacitación en ciberseguridad para funcionarios públicos	**No cumplida**	No hay un levantamiento y catastro formal de oferta de capacitación para funcionarios y debidamente publicado en un sitio web accesible por el público objetivo o bien mecanismo de difusión.
38	Acuerdo de Budapest	**Cumplida**	Durante abril del año 2017, el congreso promulga el Convenio sobre la Ciberdelincuencia ***https://bcn.cl/2ij3n***, instrumento de adhesión de la República de Chile al convenio de Budapest suscrito desde noviembre del 2001. El 12 de mayo del 2022 nuestro país firmó el Segundo Protocolo, en el marco de la conferencia internacional sobre cooperación reforzada y divulgación de pruebas electrónicas. El paso siguiente es comenzar el trabajo para la ratificación del Segundo Protocolo, incluyendo las reservas y declaraciones que el Gobierno de Chile estime necesario incluir. Al respecto, tanto el Ministerio del Interior como el Ministerio de Justicia han informado al Ministerio de Relaciones Exteriores sobre sus respectivas propuestas (en particular respecto a los artículos 7 y 8 del texto), a objeto de que sean analizadas por DIGEJUR.
39	Patrocinio de proyectos de I+D en ciberseguridad	**No cumplida**	No se presentaron avances en esta medida. Se ha consultado mediante oficio al Ministerio de Ciencia por proyectos de I+D sobre ciberseguridad, el cual se encuentra en espera de respuesta.
40	Mesa formación capital humano avanzado en ciberseguridad	**Cumplida**	Respecto de la medida N°40, se han desarrollado las siguientes actividades: • 2019 (18 pfc-99573): programa de formación para la seguridad de la información y la ciberseguridad, con el objetivo de generar competencias en materia de seguridad de la información y ciberseguridad en trabajadores que se desempeñen laboralmente en pequeñas y medianas empresas (pymes) y cuyo negocio implique un uso intensivo de sistemas digitales de información. • 2022 (22 pfc-201213): formación para siete perfiles laborales TIC de especialidad 2022: formar capital humano especializado en los perfiles de data analyst (análisis de datos), *data scientist* (ciencia de datos), arquitectura cloud, especialización devops, especialización IoT, ciberseguridad y *lean-agile business developer*, desarrollando acciones que permitan masificar estas temáticas.
41	Apoyar exportación de productos y servicios de ciberseguridad	**No cumplida**	Se desconocen antecedentes sobre el trabajo de PROCHILE y/o MINECON en esta materia.

El siguiente es un resumen de lo que se logró en el objetivo de cooperación internacional:

1. La Subsecretaría de Relaciones Exteriores desplegó una agenda extensa de medidas tanto en el contexto de la OEA como de las Naciones Unidas, destinadas a fomentar la cooperación y confianza en el ciberespacio, para fomentar avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, para contrarrestar el uso indebido de las TICs con fines delictivos, y otros (medidas 23 y 24).

2. El acuerdo de Budapest ya mencionado (medida 38) permitirá fortalecer la compartición de información acerca de incidentes de seguridad, ocurridos en instituciones de nuestro país, con los Centros de Respuesta a Incidentes Informáticos de otros países.

3. Las medidas de formación de profesionales informadas por CORFO (medida 40), especialmente la referida a perfiles técnicos avanzados, ayudan a establecer relaciones de pares profesionales con expertos extranjeros de organizaciones como FIRST.

En este objetivo hubo medidas que no fueron cumplidas: no se elaboró un documento de política internacional en ciberseguridad para nuestro país (medida 25), no se concretó la generación de grupos internacionales para propiciar el compartir experiencias entre representantes de países de Latinoamérica sobre ciberseguridad (medida 26), ni se apoyó la exportación de productos y servicios nacionales en ciberseguridad (medida 41). Se recomendará que algunas de estas medidas sean incorporadas en la nueva Política.

3.5. PROMOCIÓN DE INDUSTRIA

Finalmente, en la siguiente tabla aparece el detalle de cada una de las medidas y su avance dentro de este objetivo:

#	MEDIDA	ESTADO	DESCRIPCIÓN DEL CUMPLIMIENTO
28	**Informe sobre regulación de compras públicas**	**Cumplida**	La Dirección de Compras y Contratación Pública, en adelante e indistintamente "ChileCompra", para llevar a cabo dicho compromiso, realizó un análisis previo de acuerdo con su función asesora contemplada en el artículo 30, letra a), de la Ley N° 19.886, y sus facultades contenidas en el artículo 104 bis del reglamento del citado cuerpo legal. En tal sentido, la Dirección ha elaborado una serie de Directivas de Contratación que contienen recomendaciones y buenas prácticas cuya adhesión, tanto por parte de los organismos públicos como por parte de los proveedores, favorece una mejor gestión de los procesos de compra, dentro del marco legal vigente. Se pueden destacar, entre otras, las siguientes directivas a partir de las cuales se advierte que la regulación y aplicación del régimen vigente de compras públicas resulta pertinente para el apoyo productivo en materia de ciberseguridad, de forma concordante con intereses nacionales estratégicos: • Directiva de Contratación Pública N°22 sobre "Orientaciones sobre la participación de las Uniones Temporales de Proveedores en los procesos de Compra". • Directiva de Contratación Pública N°38 sobre "Recomendaciones para la contratación de bienes y servicios relacionados con tecnologías de información" • Directiva de contratación Pública N°33 sobre "Recomendaciones para la innovación en las compras públicas"
29	**Estudios de industria nacional de ciberseguridad**	**Cumplida**	En relación con la medida N°29, la Corporación financió un estudio sobre "Consultoría experta en la elaboración del diseño de la metodología para evaluar el grado de madurez en seguridad informática de organismos del Estado y de sectores industriales relevantes en materia de ciberseguridad", contratado mediante Resolución Exenta N°1941, de 30 de diciembre de 2016, con la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile. No obstante, de acuerdo con la cláusula duodécima del contrato suscrito entre las partes, el informe final de dicho estudio quedó en poder de la Agencia Nacional de Inteligencia, para su posterior análisis.

#	MEDIDA	ESTADO	DESCRIPCIÓN DEL CUMPLIMIENTO
30	Estudio de incentivos para estándares de ciberseguridad	Cumplida	La reforma tributaria incorpora un nuevo artículo 20 bis a la Ley de Impuesto a la Renta, la cual establece una tasa de desarrollo ascendente a un 2%, adicional a la tasa de primera categoría de la Ley de Impuesto a la Renta, aplicable a las empresas que determinen su renta efectiva en base a contabilidad completa según lo indicado en el artículo 14 A. La base imponible sobre la cual se aplica el impuesto corresponde a la diferencia entre el 2% de la renta líquida imponible del ejercicio y la suma de los desembolsos efectuados por el contribuyente, dentro del ejercicio, que califique como inversión en productividad. Al respecto, la nueva norma indica que se entiende como inversión en productividad: *"Los desembolsos destinados a la preparación y presentación de solicitudes de protección de propiedad industrial, así como los gastos legales asociados a la defensa de estos derechos una vez adquiridos, siempre que el bien objeto de protección se haya producido o inventado en Chile. Cumpliendo los mismos requisitos se podrán considerar los desembolsos de preparación, presentación y defensa de propiedad industrial efectuados en el extranjero".* *"Los desembolsos destinados a obtener certificaciones ISO".* En consecuencia, los contribuyentes que inviertan en actividades o productos tendientes a aumentar o mejorar sus políticas o programas de ciberseguridad, podrán descontar los mismos de la base imponible de la mencionada tasa de desarrollo, lo que genera un incentivo para la contratación de este tipo de servicios.
35	Estándares de ciberseguridad para proveedores del Estado	Cumplida	Para llevar a cabo dicho compromiso, la Dirección de Compras y Contratación Pública ha preparado recomendaciones generales para los compradores públicos, para que sean ellos, a partir de sus respectivos requerimientos de compra, formalizados en las bases de licitación o en el requerimiento de un trato directo, sea quienes exijan el cumplimiento de estándares de ciberseguridad por parte de los oferentes, dentro de la normativa vigente. Se actualizaron los términos y condiciones de uso de la plataforma ***www.mercadopublico.cl*** para establecer las responsabilidades de los proveedores y compradores en el uso de cuentas de acceso, se actualizaron los requerimientos hardware y software (PC, aplicaciones y sistema operativo) para prevenir vulnerabilidaddes, malware y otras amenazas, a través de la Resolución Exenta N° 585-B, de 02 de septiembre del 2021, de la Dirección de Compras y Contratación Pública, la cual "Aprueba nuevas políticas y condiciones de uso del sistema de Información de compras oúblicas y registro de proveedores" ***https://www.chilecompra.cl/wp-content/uploads/2021/09/585-B-Res.-Aprueba-Nuevas-Politicas-y-Condiciones-de-uso.pdf***
41	Apoyar exportación de productos y servicios de ciberseguridad	No cumplida	Se desconocen antecedentes sobre el trabajo de PROCHILE y/o MINECON en esta materia.

Este objetivo tuvo un alto nivel de cumplimiento, siendo cuatro medidas de las cinco, implementadas por sus responsables.

Solo la medida 41, "Apoyar exportación de productos y servicios de ciberseguridad", no se cumplió. Se evaluará considerarla nuevamente en la nueva Política con el objetivo de reforzar el crecimiento de la industria, entregando herramientas para robustecer las acciones que se tomen en materia de ciberseguridad.

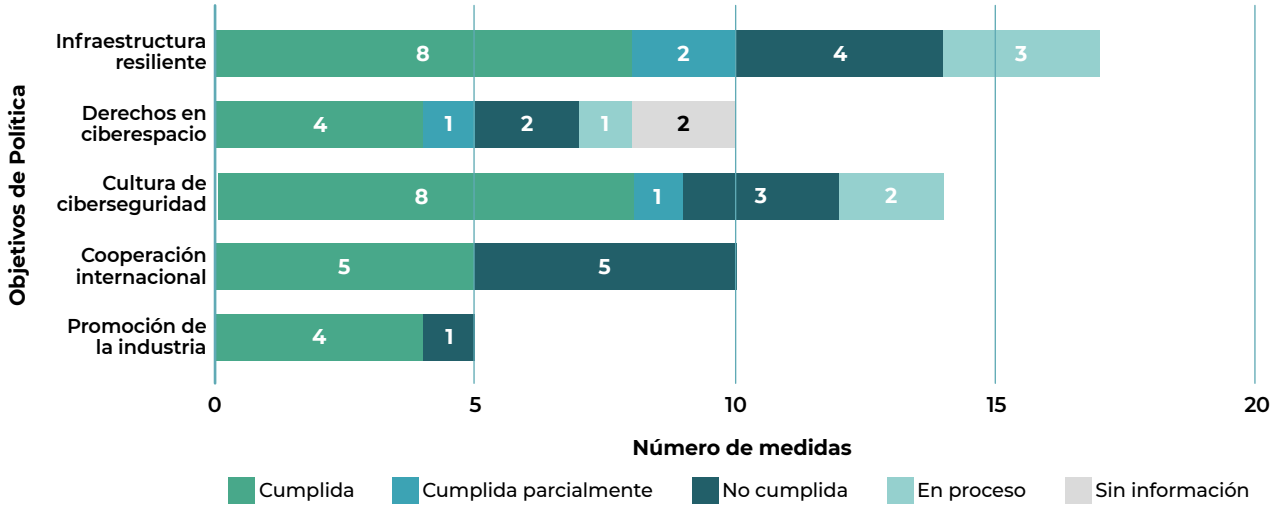
4. EVALUACIÓN DE LAS MEDIDAS

AVANCE DE LAS MEDIDAS

En términos generales, es indudable que en el ámbito de la ciberseguridad el país está mejor hoy que hace cinco años, al menos en los primeros cuatro de los cinco objetivos planteados en la Política Nacional de Ciberseguridad. Sin embargo, como debiera ser evidente, existe todavía un gran número de desafíos a superar en los próximos años.

El gráfico en la figura 1 (abajo) muestra el número de medidas cumplidas en cada uno de los objetivos. Cada barra indica el número de medidas en cada categoría ("Cumplida", "Cumplida parcialmente", "No cumplida", "En proceso" y "Sin información"). El gráfico sólo pretende orientar acerca del número de medidas; el "tamaño" o dificultad de implementación de las medidas pueden ser muy distintas entre sí. Dado que algunas medidas fueron consideradas como contribuyendo a más de un objetivo, la cantidad de medidas suma más que 41.

FIGURA 1
Número de medidas por cumplimiento en Política Nacional de Ciberseguridad (PNCS) 2018-2022



Fuente: Unidad de coordinación de ciberseguridad, Subsecretaría de Interior.

En términos de cantidad de medidas, el mayor nivel de cumplimiento se observa en los objetivos primero y tercero, a saber: **Infraestructura resiliente** ("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") y **Cultura de ciberseguridad** ("Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales").

Respecto al primer objetivo (**infraestructura resiliente**), existen dos aspectos relacionados con la resiliencia[6]:

1. **La capacidad de las redes de Internet en nuestro país para soportar las fallas físicas.** En la mayor parte de los casos en el pasado estos problemas se han debido a desastres socioambientales (como el terremoto de 2010[7]); una de las posibilidades que tenemos que considerar en el futuro es que estas redes pudieran ser atacadas físicamente de forma intencional, tanto en tierra como en el mar (por ejemplo, cortando o interviniendo la fibra óptica que llega al país a Arica o a Valparaíso).

   Hoy, gracias al estudio realizado por Subtel y NIC Chile (medida 12), conocemos mejor el estado de la conectividad en el país. Sin embargo, hay varias comunas en Chile que todavía no tienen una conexión de alta velocidad y estable; las condiciones topográficas de nuestro país dificultan el llegar a estos lugares, y factores como el clima pueden dificultar grandemente la comunicación con ciertos lugares, especialmente en el extremo sur. El desafío en el futuro cercano es lograr resiliencia de conexión no sólo conectando todos las ciudades y pueblos de Chile, sino teniendo al menos dos conexiones a cada lugar para minimizar la probabilidad de que una localidad quede aislada por desastre socioambiental o por ataque intencional.

2. **La capacidad de los sistemas informáticos que proveen servicios esenciales para resistir ataques dirigidos.** Estos ataques son principalmente de dos tipos: ataques técnicos o engaños de ingeniería social. El primer tipo se refiere al acceso no autorizado a sistemas informáticos a través de vulnerabilidades técnicas, o haciendo abuso de errores cometidos por personas. Estas vulnerabilidades o errores permiten a atacantes tomar el control total o parcial de los sistemas (con lo que pueden montar otros ataques), exfiltrar información sensible (por la que pueden intentar extorsionar a las instituciones), o bien modificar o destruir información (lo que puede ser políticamente motivado).

   Muchas instituciones tienen hoy una preparación incipiente para responder frente a incidentes de ciberseguridad (ciertamente mejor que hace cinco años atrás). Los avances en control de gestión (medidas 6, 9 y 10), las actividades regulares del CSIRT (medida 34), y los avances normativos o técnicos descritos anteriormente (medidas 1, 5 y 7), sumados a otras normativas que tienen relación con seguridad de la información pero que no fueron parte de la Política representan, en su conjunto, un avance importante con respecto a la situación del país hace cinco años atrás, pero no son suficientes; es necesario adaptarse a circunstancias nuevas y cambiantes.

[6] El término "resiliencia" tiene varios significados técnicos ligeramente distintos, dependiendo del contexto. Resiliencia es la capacidad de una organización para resistir al ser afectado por disrupciones (ISO(IEC) 27031:2011 (en), Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity; "3.14 Resilience: ability of an organization to resist being affected by disruptions"); si se trata de sistemas informáticos, resiliencia es la habilidad de un sistema para soportar y recuperarse rápidamente de una falla (ISO/IEC TR 15067-3-8:2020 (en), Information technology — Home Electronic System (HES) application model — Part 3-8: GridWise transactive energy framework; "3.24 resilience: ability to resist failure and rapidly recover from a breakdown").

[7] Ver la charla de José Miguel Piquer, director de investigación de NIC Chile: *https://www.youtube.com/watch?v=pk7fEVEevhA*. Consultada el 26 de enero de 2023.

Respecto al tercer objetivo (**Cultura de ciberseguridad**), son muy variados los factores que influyen en éste. En el modelo de madurez de capacidades en ciberseguridad (Cyber Security Capability Model, o CMM) de la Universidad de Oxford[8], la formación de una cultura de ciberseguridad está asociado a dos grandes factores (ver figura 2):

1. Cultura cibernética y Sociedad (D2): Se relaciona con fomentar una cultura de ciberseguridad responsable en la sociedad, asociado a los siguientes subfactores:

   a. Mentalidad de ciberseguridad (D2.1)
   b. Confianza y seguridad en Internet (D2.2)
   c. Comprensión del usuario en la protección de información personal en línea (D2.3)
   d. Mecanismos de denuncia (D2.4)
   e. Medios y redes sociales (D2.5)

2. Formación, Capacitación y Habilidades de Seguridad Cibernética (D3): Se relaciona con el desarrollo del conocimiento de ciberseguridad, y está asociado a los siguientes subfactores:

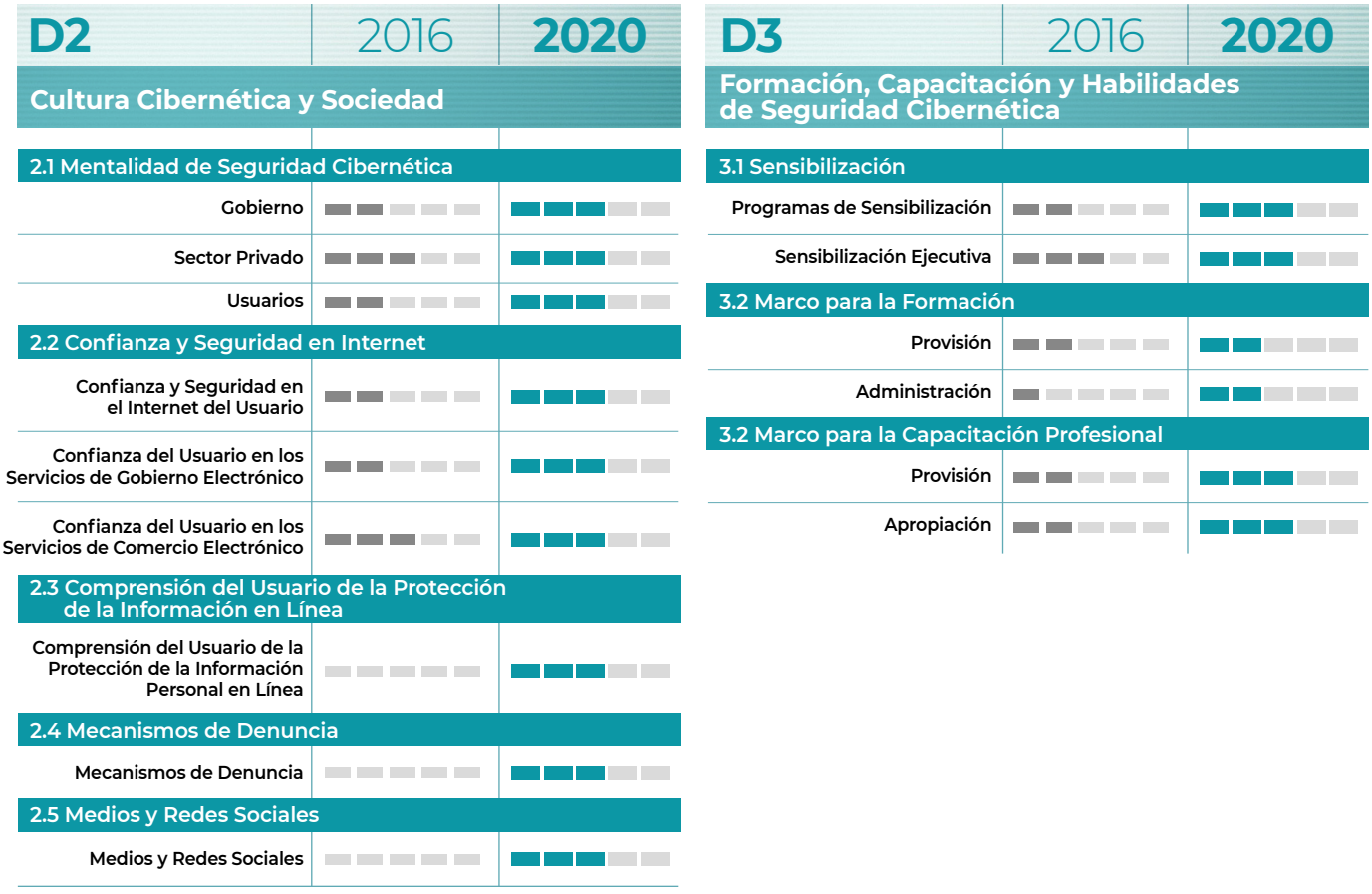
   a. Sensibilización (D3.1)
   b. Marco para la educación (D3.2)
   c. Marco para la formación profesional (D3.3)

[8] El modelo de madurez de ciberseguridad (Cybersecurity Capacity Maturity Model, o CMM) es mantenido por el Global Cyber Security Capacity Centre, dependiente de la Universidad de Oxford, y es un modelo de referencia internacional conocido y aplicado mundialmente para medir la madurez (esto es, la capacidad progresiva) de los países en materia de ciberseguridad. Ver ***https://gcscc.ox.ac.uk/the-cmm***; consultado el 25 de enero de 2023.

Las medidas reportadas anteriormente sobre cultura de la ciberseguridad (medidas 16, 17, 18, 19, 20, 21, 34, 36 y 40) aportan a los tres primeros sub-factores de D2 (D2.1 hasta D2.3), y al subfactor D3.1. Algunas medidas incluidas en otros objetivos (directamente, las medidas 13, 14 y 15, e indirectamente las medidas 36 y 38) contribuyen al subfactor D2.4. Lo anterior implica que aun habiendo avanzado mucho, no hubo medidas que contribuyeran a los factores D3.2 (marco para la educación), D3.3 (marco para la formación profesional) y D2.5 (medios y redes sociales).

La educación en ciberseguridad es probablemente una de las medidas más efectivas (pero también más difíciles) que se puede acometer como país para lograr un cambio real y duradero en términos de la conciencia de las personas acerca de la importancia de la ciberseguridad, y de la generación de hábitos de protección de los datos personales.

FIGURA 2
Resultados de la evaluación de Chile en 2016 y 2020[9] en las dimensiones 2 y 3 del modelo de madurez de capacidades en ciberseguridad (CMM) de la Universidad de Oxford.

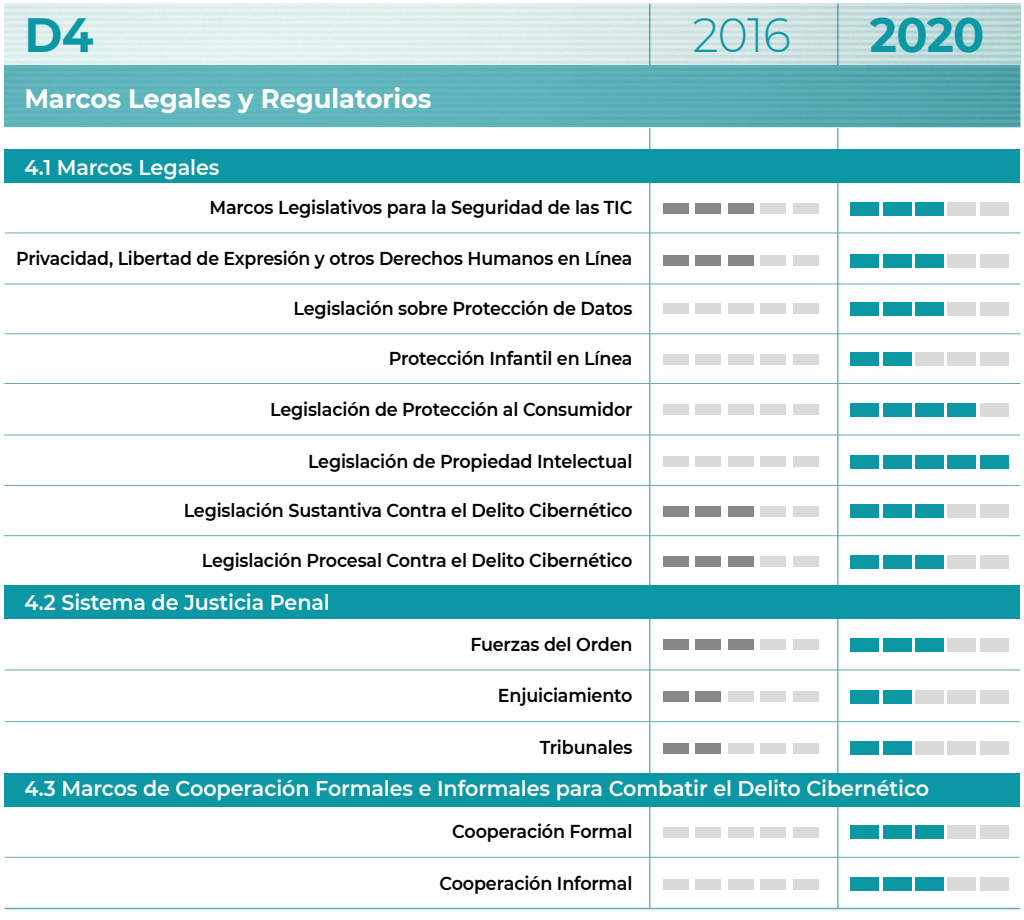


[9] La Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) aplicaron el CMM en toda Latinoamérica y el Caribe en 2016 y luego en 2020. Los resultados de ambos años pueden ser consultados de forma interactiva en el sitio *https://cybersecurityobservatory.org/*. Consultado el 25 de enero de 2023.

En términos de los objetivos restantes, en el segundo objetivo (**Derechos de las personas en el ciberespacio**) es donde probablemente tenemos el mayor espacio para avanzar. El avance es el mismo mencionado en el factor D2.4 (medidas 13, 14, 15, 36 y 38); falta la promulgación de la mejora de la Ley de Protección de Datos Personales (medida 31), que ha estado años en discusión parlamentaria, y falta la promulgación de ley marco de ciberseguridad (medida 1). Falta asimismo trabajar en el resto de las dimensiones incluidas en el cuarto factor del modelo CMM (ver figura 3): protección infantil en línea y protección al consumidor. Sin embargo, en junio de 2022 se promulgó la ley 21.459, que deroga la ley de delito informático y propone nuevos tipos penales, de acuerdo con el Acuerdo de Budapest firmado por nuestro país.

FIGURA 3

Resultados de la evaluación de Chile en 2016 y 2020 en la dimensión 4 del modelo de madurez de capacidades en ciberseguridad (CMM) de la Universidad de Oxford



Finalmente, el menor nivel de cumplimiento se puede observar en el quinto objetivo, Fomento a la industria de ciberseguridad. Se recomendará fuertemente incluir acciones en la próxima política que tengan al Estado como un facilitador e incentivador del surgimiento y sofisticación de la industria de ciberseguridad.

ASPECTOS TRANSVERSALES

Una parte fundamental de los derechos en línea, que no estuvieron presentes en la Política y que deben ser incorporados dado el avance que hemos tenido como sociedad en los últimos años, es la perspectiva de género, entre otros aspectos transversales. Para analizar este tema en la Política se contrató una consultoría. Una de las conclusiones es que el tema casi no es mencionado en la Política, y fue escasamente considerado tanto en el desarrollo como en la implementación de medidas. Esto sólo se justifica por el momento social específico en que fue escrito el documento (2016-2017). La consultora concluye que el reto de la próxima Política Nacional de Ciberseguridad 2023-2028 será incorporar de forma transversal el enfoque de género. Para eso, será necesario trabajar con todas las partes interesadas para comprender las brechas de género más urgentes de las que la política debe hacerse cargo, además de identificar las oportunidades que en Chile existen para apalancar el avance de la perspectiva de género en la ciberseguridad. Las condiciones para que el país siga siendo pionero en el enfoque de género en la ciberseguridad están plenamente dadas.

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

INFORME DE IMPLEMENTACIÓN

POLÍTICA NACIONAL DE CIBERSEGURIDAD

2017-2022

CICS Comité Interministerial sobre Ciberseguridad

Sistema Nacional de CIBERSEGURIDAD