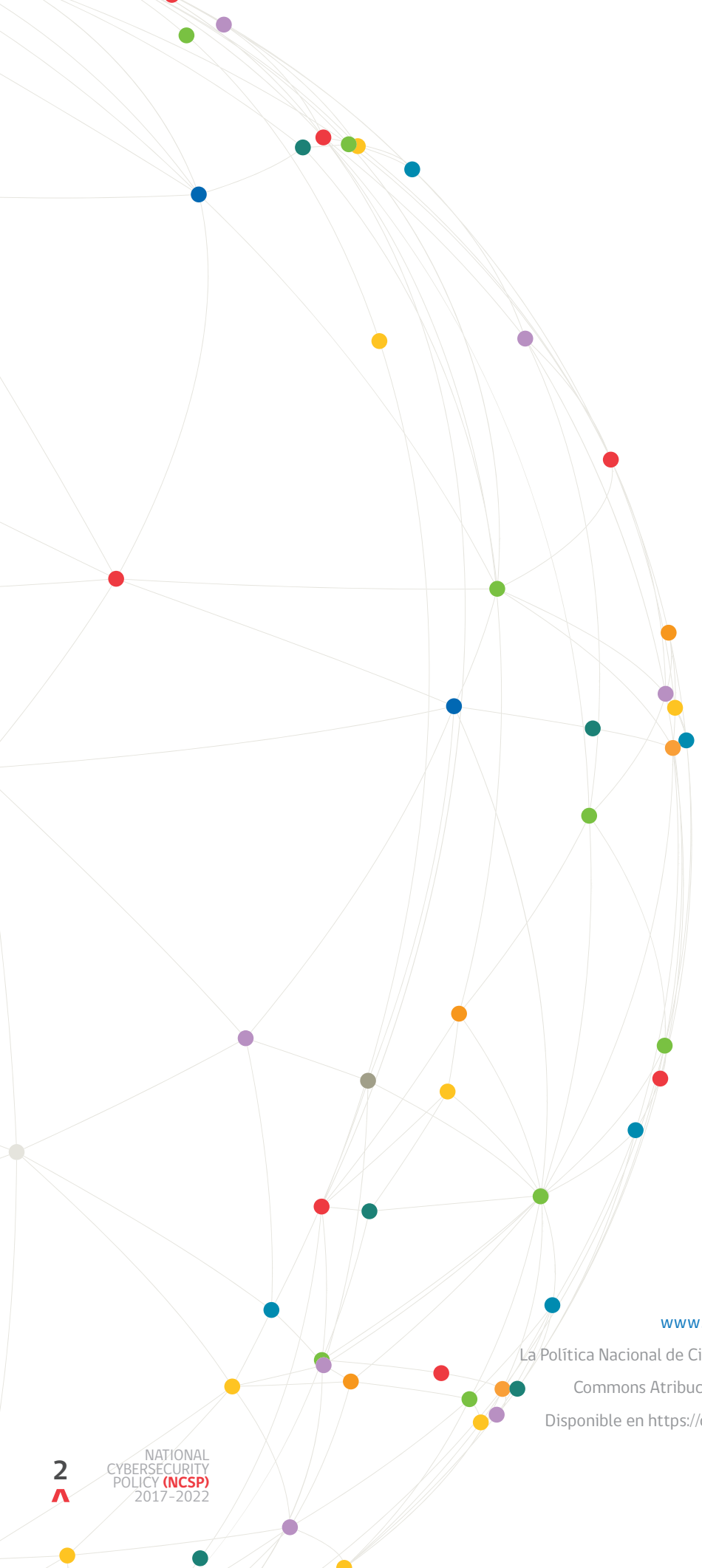
POLÍTICA NACIONAL DE CIBERSEGURIDAD

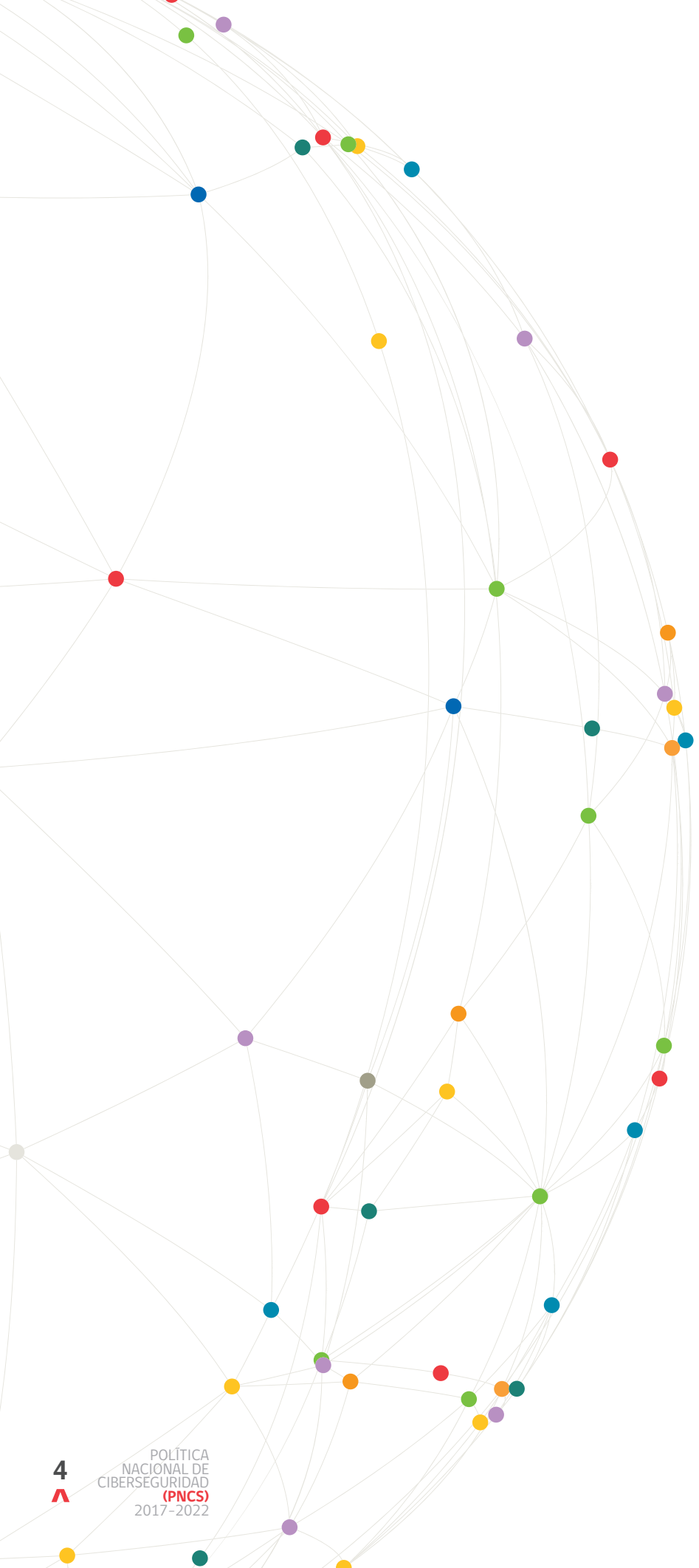
Gobierno de Chile

www.gob.cl



www.ciberseguridad.gob.cl

Índice



Una Política de Ciberseguridad para Chile

Las Tecnologías de la Información y la Comunicación (TIC) son una herramienta sin parangón en la historia para las personas, para las interacciones institucionales, los trámites, las operaciones económicas y las comunicaciones privadas y públicas.

Su impacto ha sido profundo en nuestra sociedad y se extiende día a día. Los accesos a internet han crecido en un 45,3%, en el último bienio, pasando de 52,2 accesos por cada 100 habitantes a inicios de 2014, a 73,8 accesos por cada 100 habitantes en marzo de 2016. La economía digital nacional, en tanto, creció en torno al 11% en el último bienio, pasando de 34.127 millones de dólares en 2014 a 39.485 millones de dólares en 2015.

Este impacto ha generado trasformaciones relevantes también en los usos y miradas de nuestros ciudadanos.

Las TIC tienen un efecto social sin precedentes, permitiendo, entre otros usos, que las ciudadanas y ciudadanos se informen, organicen y participen a través de internet y particularmente que nuestras niñas, niños y adolescentes realicen un uso intensivo de las denominadas redes sociales.

Una transformación de esta magnitud no puede sino implicar desafíos importantes para el Estado, pues es imperativo poner esta potencialidad tecnológica al servicio de las personas y de la convivencia social. Para ello necesitamos democratizar el uso de internet y transformarla en un campo de inclusión, de eficiencia, y de certezas, custodiando la seguridad y la privacidad de quienes usan la red cotidianamente.

De cara a este desafío, Chile debe ponerse al día en materia de seguridad, porque cualquier error o ataque exitoso puede vulnerar el bienestar y los derechos de chilenas y chilenos, afectar intereses particulares y comunes, afectar servicios críticos para el funcionamiento del país.

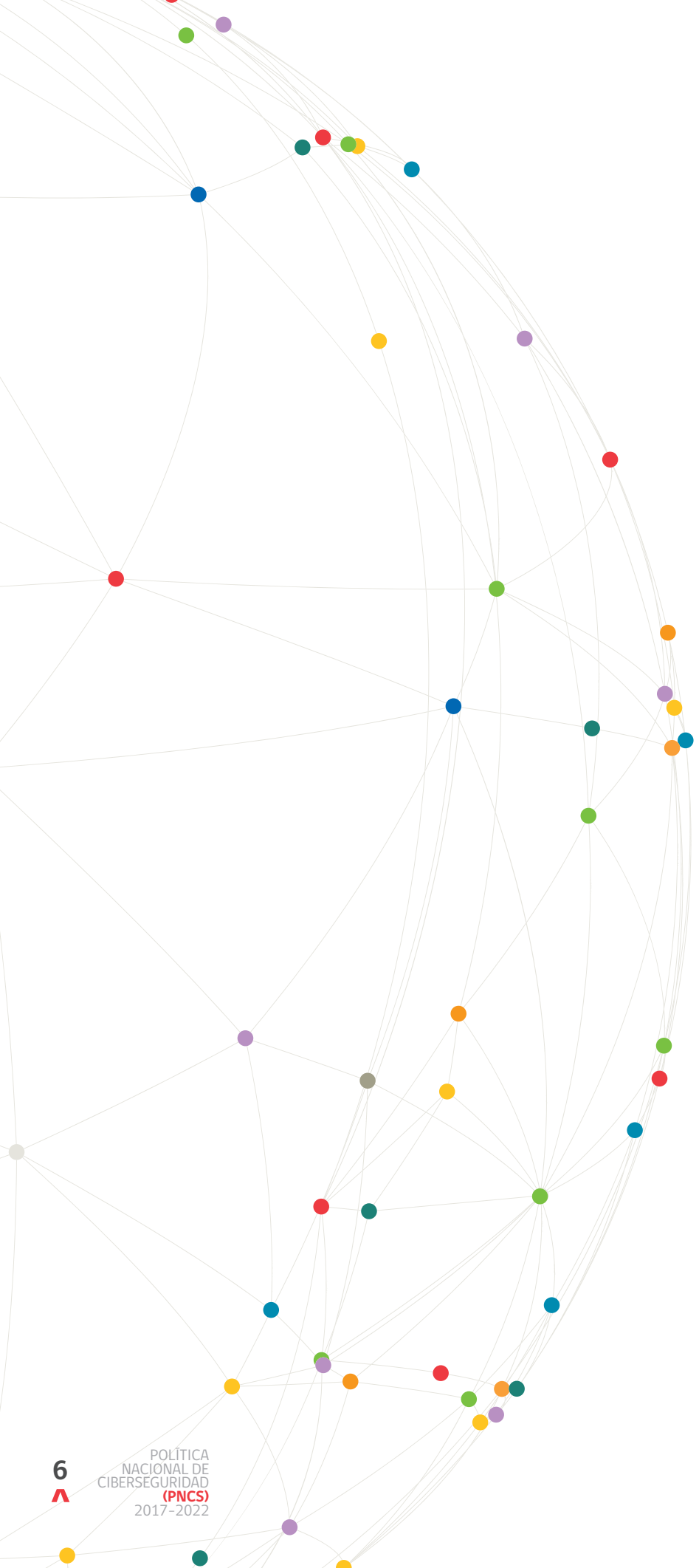
Atendiendo a esta exigencia, mi programa de gobierno consideró el desarrollo de una estrategia de seguridad digital, para proteger a usuarios privados y públicos en el ámbito digital.

Este compromiso fue refrendado en noviembre del 2015, cuando presentamos la Agenda Digital 2020, que considera especialmente la necesidad de elaborar una estrategia de ciberseguridad, plasmada en este documento.

Esta primera Política Nacional fue construida a partir de un intenso diálogo público privado. Durante meses se recibió en audiencia pública a representantes de servicios públicos, de organizaciones gremiales y de la sociedad civil, además de académicos y expertos nacionales e internacionales. Luego, cuando el Comité Interministerial elaboró el primer borrador de la Política, se sometió al proceso de consulta pública que establece la ley N°20.500 sobre participación de la sociedad civil, donde se recibieron numerosas contribuciones que sin duda ayudaron a mejorar la propuesta.

La Política Nacional plantea metas y compromisos concretos con el objetivo de promover un ciberespacio libre, abierto, seguro y resiliente. Un espacio de seguridades que permita a las chilenas y chilenos alcanzar el mayor desarrollo posible. En línea con la Agenda Digital y la Agenda de Productividad, Innovación y Crecimiento, permitirá reducir las brechas de acceso y la conciencia sobre el uso seguro de las TIC y aprovechar las enormes ventajas que tiene nuestro país debido a su posición de liderazgo en el ámbito tecnológico en la región.

Michelle Bachelet Jeria
Presidenta de la República



La penetración de las TIC en todas las áreas en las que nos desarrollamos y relacionamos ha significado una revolución que no ha dejado a nadie indiferente. En la actualidad nos cuesta pensar en una vida sin las redes informáticas y eso incluye, por cierto, nuestras relaciones sociales.

En el ámbito público, la administración del Estado en forma creciente coloca información e interactúa con los ciudadanos a través de internet, cumpliendo de este modo compromisos de oportunidad en la entrega de sus servicios y transparencia en su gestión, promoviendo de esta forma el gobierno digital. Junto a lo indicado y con la finalidad de facilitar el acceso de internet a la ciudadanía, el Estado ha generado programas de libre acceso, ello a través del programa WiFi ChileGob, proyecto que ayuda a mejorar el acceso en los lugares más vulnerables de Chile que poseen pocas alternativas de conectividad. Adicionalmente, el gobierno impulsa la iniciativa Yo elijo mi PC, que busca aumentar los niveles de equidad y disminuir la brecha digital, favoreciendo a niños y niñas en condición de vulnerabilidad de séptimo año básico. Así, en los siete años que lleva el programa, se ha beneficiado a más de 350.000 estudiantes.

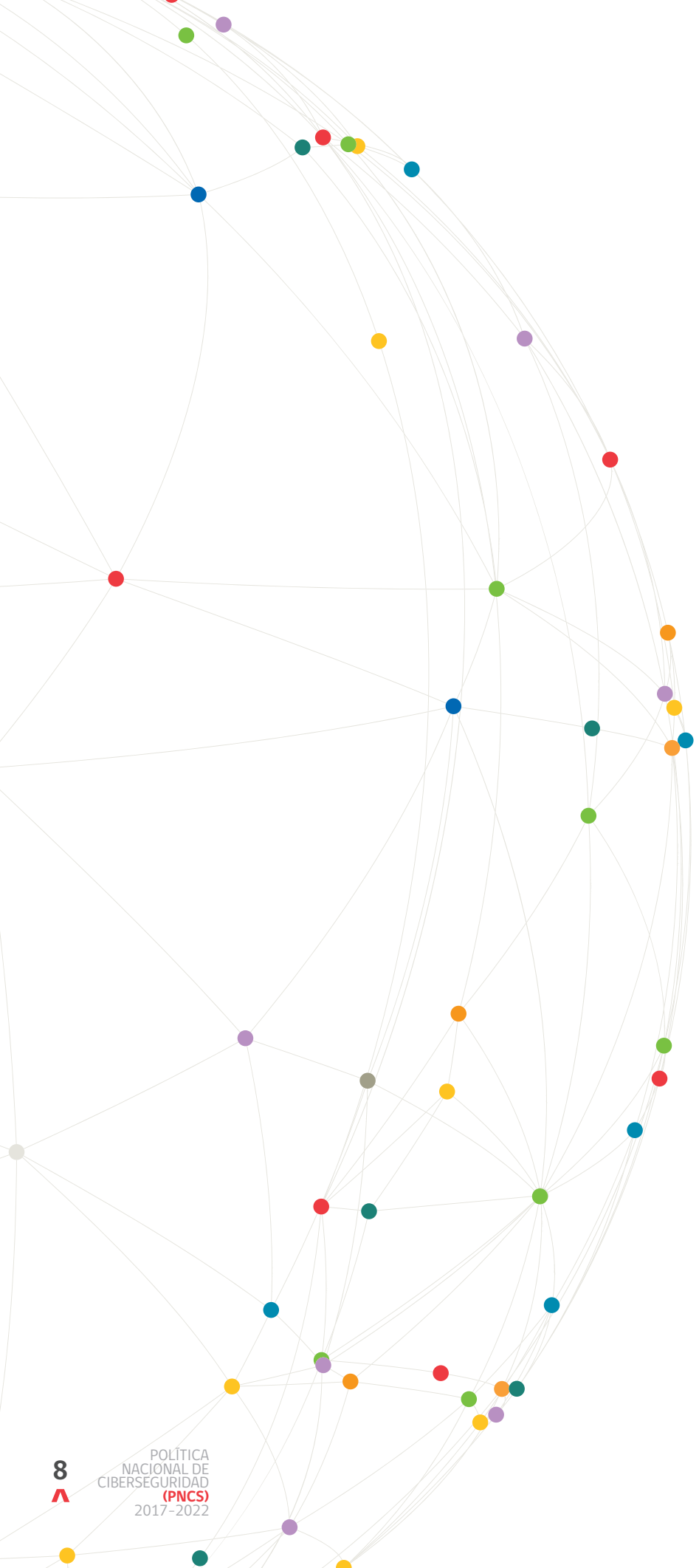
En el contexto anterior, donde el acceso a internet y el uso y dependencia de las TIC aumenta ostensiblemente, el fenómeno criminológico asociado al cibercrimen y a los ataques cibernéticos se ha visto potenciado. Así, por ejemplo, la Red de Conectividad del Estado registró un aumento en los patrones maliciosos que la afectan de más de cien millones de ataques, entre 2014 y 2015, pasando el año 2016 a cifras exponelcialmente más altas por ataques de Denegación Distribuida de Servicios (DDoS).

Ante tal realidad, tanto el programa de gobierno de la presidenta Michelle Bachelet como la Agenda Digital 2020 consideran especialmente el desarrollo de una estrategia de seguridad digital que promueva la protección de los usuarios privados. Por lo anterior, el gobierno ha trabajado desde abril del año 2015, mediante un Comité Interministerial de Ciberseguridad, en la elaboración de esta, la primera Política Nacional de Ciberseguridad del país, la cual ha sido afinada luego de un exitoso proceso de Consulta Ciudadana llevado a cabo entre febrero y marzo del año 2016.

Si bien la Política Nacional de Ciberseguridad aborda con especial interés la persecución y sanción de los ciberdelitos, su espíritu va mucho más allá del ámbito punitivo, ya que una variable fundamental para disminuir los riesgos asociados al ciberespacio y aprovechar sus potencialidades es la sensibilización, formación y difusión en ciberseguridad de la ciudadanía. Asimismo, aprovechando las ventajas competitivas que tiene nuestro país en términos de acceso a internet, madurez del mercado digital y calidad de los profesionales, la Política busca promover el desarrollo industrial y productivo en ciberseguridad.

De esta forma, estoy convencido de que las medidas que se implementarán con ocasión de la Política de Ciberseguridad así como los lineamientos de Estado que ésta contempla contribuirán a un mayor desarrollo de la cooperación interinstitucional y público-privada, lo que permitirá relevar el valor de un ciberespacio libre, abierto y seguro, como una vía para lograr un mayor desarrollo económico de nuestro país y un mayor bienestar para las chilenas y chilenos.

Mahmud Aleuy Peña y Lillo
Subsecretario del Interior
Presidente, Comité Interministerial sobre Ciberseguridad



Hace bastante tiempo que el ciberespacio dejó de ser parte de la ciencia ficción para convertirse en uno de los principales espacios de interacción social. Sin ir más lejos, Chile ostenta la mayor tasa de penetración de internet en América Latina, con más de un 70% de su población conectada.

Esto ha permitido que los habitantes de nuestro país utilicen intensivamente las tecnologías digitales para comunicarse entre sí, para expresar sus ideas, compartir sus causas o estrechar vínculos personales a través de las redes sociales, para realizar múltiples trámites en línea y, también, para aprovechar las ventajas del comercio electrónico. Sin embargo, esta utilización intensiva incrementa también nuestros niveles de dependencia de la red y de la infraestructura que la soporta, así como nos expone a nuevos riesgos y amenazas.

Por ello, uno de los desafíos que asumimos como Gobierno fue mejorar los estándares de seguridad digital de nuestro país, con el fin de proteger a las personas y el ejercicio de derechos fundamentales como la privacidad, la libertad de expresión y el acceso a la información, entre otros.

La presente política constituye el primer resultado concreto de ese desafío, resultado que es fruto del trabajo colectivo que asumimos en el Comité Interministerial sobre Ciberseguridad, integrado por las Subsecretarías de Interior, Relaciones Exteriores, Defensa, Hacienda, Secretaría General de la Presidencia, Economía, Justicia, Telecomunicaciones y la Agencia Nacional de Inteligencia. El Comité sesionó durante todo el año 2015, convocando a múltiples audiencias públicas donde recibió a representantes de entidades gremiales, de empresas, de organizaciones de la sociedad civil, académicos y expertos nacionales e internacionales en ciberseguridad.

Esta Política fue objeto de un extenso proceso de consulta pública, en el cual se recibieron medio centenar de observaciones, comentarios y críticas que, por cierto, enriquecieron el documento que ustedes tienen en sus manos.

La Política plantea cinco objetivos estratégicos de largo plazo, destinados a abordar los desafíos que como país enfrentamos ante el ciberespacio, incorporando no sólo el ámbito de acción del Estado, sino también considerando el rol que la cabe al sector privado, la sociedad civil y el mundo académico en esta importante tarea.

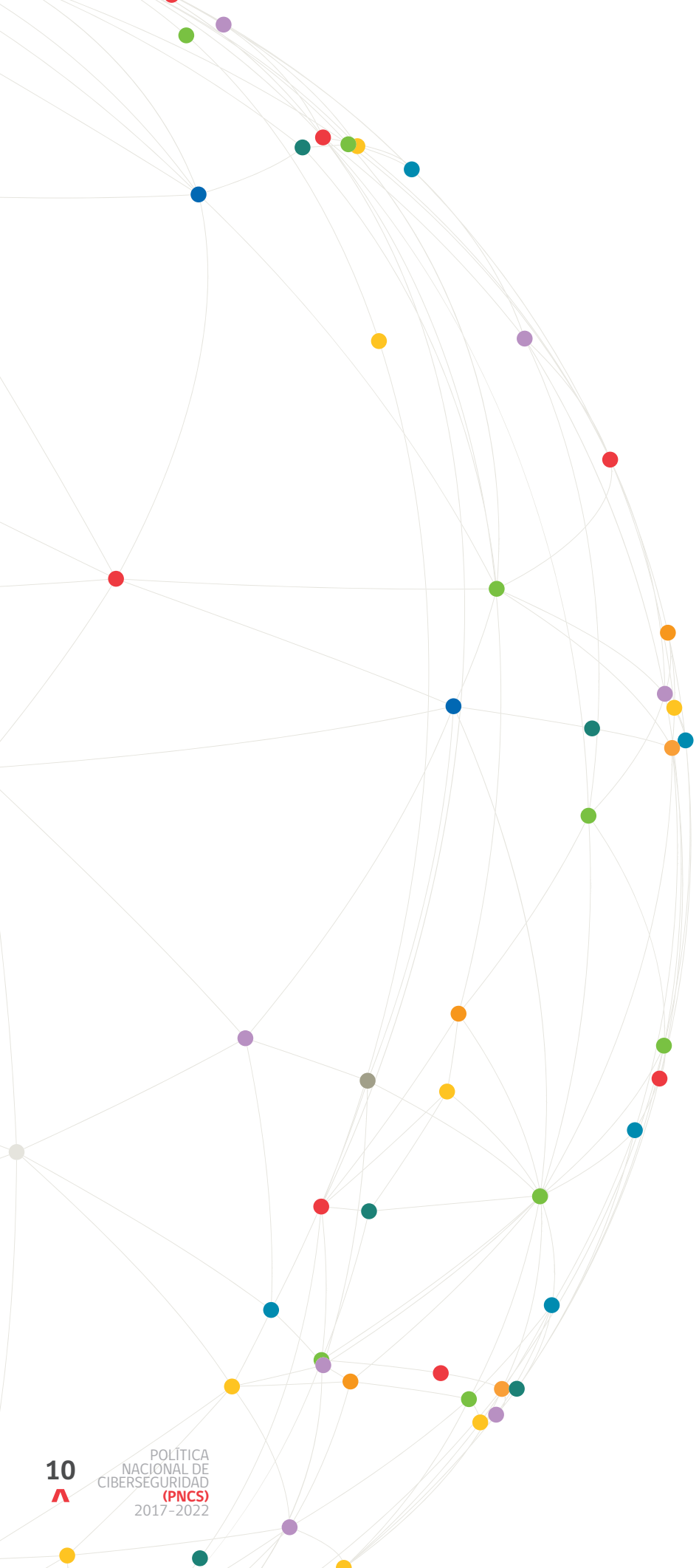
La Política refleja una idea central para los tiempos que corren: seguridad y libertad son conceptos complementarios entre sí, y el combate a los ciberdelitos y otras amenazas en Internet no puede convertirse en una excusa para atropellar derechos humanos como la privacidad y la libertad de expresión, sino un modo de garantizar plenamente estos derechos en el ciberespacio.

Ahora enfrentamos el gran desafío de implementar la Política y monitorear su efectividad, para lo cual resulta imprescindible contar con la colaboración de todos los actores involucrados, de manera que nuestro país siga avanzando en la construcción de un ciberespacio abierto, libre y seguro para todos y todas.

Marcos Robledo Hoecker

Subsecretario de Defensa

Secretario Ejecutivo, Comité Interministerial sobre Ciberseguridad



2 Introducción

La masificación en el uso de tecnologías de información y comunicaciones (TIC), junto con servir al desarrollo del país, conlleva riesgos que pueden afectar los derechos de las personas, la seguridad pública, las infraestructuras críticas, el gobierno digital, los intereses esenciales y la seguridad exterior de Chile.

Estos riesgos pueden provenir de múltiples fuentes y se pueden manifestar mediante actividades de espionaje, sabotaje, fraudes o ciberataques realizados por otros países, por grupos organizados o por particulares, entre otros.

A nivel internacional existe un importante desarrollo en la gestión de riesgos asociados al uso de las TIC. Al año 2015, más de 40 países contaban con una estrategia o política de ciberseguridad[1], algunos de los cuales ya están trabajando en su segunda o tercera versión. A la vez, es posible constatar la considerable evolución doctrinaria, técnica y normativa en los más diversos organismos y foros internacionales.

A nivel nacional, el desafío es contar con una política que oriente la acción del país en materia de ciberseguridad, junto con implementar y poner en marcha las medidas que sean necesarias para proteger la seguridad de los usuarios del ciberespacio, considerando estrategias educativas orientadas al autocuidado y prevención en ambiente digital, cumpliendo además con el programa de Gobierno de la Presidenta Michelle Bachelet, que propone **"desarrollar una estrategia de seguridad digital que proteja a los usuarios privados y públicos"**[2].

El presente documento contiene los lineamientos políticos del Estado de Chile en materia de ciberseguridad, con una mirada que apunta al año 2022[3], para alcanzar el objetivo de contar con un **ciberespacio libre, abierto, seguro y resiliente**.

1 Más información en los siguientes sitios web: https://ccdcoe.org/strategies-policies.html
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/
http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx

2 Programa de Gobierno de la Presidenta Michelle Bachelet, página 57.

3 Como se explica en la sección V "Hoja de ruta", esta política contiene lineamientos estratégicos de largo plazo, que apuntan a éste y el próximo gobierno, y una serie de medidas de corto plazo, que cada administración deberá planificar y ejecutar.

3 ¿Por qué se requiere una política nacional de ciberseguridad?

A. Para resguardar la seguridad de las personas en el ciberespacio

Es necesario brindar a las personas un nivel de seguridad que les permita el normal desarrollo de sus actividades personales, sociales y comunitarias en el ciberespacio, junto con el ejercicio de derechos fundamentales como la libertad de expresión, el acceso a la información, la protección de la vida privada y la propiedad.

B. Para proteger la seguridad del país

Es necesario promover el resguardo de las redes y sistemas informáticos del sector público y privado, especialmente aquellas que son esenciales para el adecuado funcionamiento del país, velando por la continuidad operacional de los servicios básicos.

C. Para promover la colaboración y coordinación entre instituciones

Es necesario mejorar las instancias de comunicación, coordinación y colaboración entre instituciones, organizaciones y empresas, tanto del sector público como privado, nacionales e internacionales, con el propósito de fortalecer la confianza y entregar una respuesta común a los riesgos del ciberespacio.

D. Para gestionar los riesgos del ciberespacio

Es necesario considerar el desarrollo de procesos de análisis y gestión de riesgos que permitan identificar las vulnerabilidades, amenazas y riesgos implícitos en el uso, procesamiento, almacenamiento y transmisión de la información, junto a la generación de las capacidades para la prevención y la recuperación ante incidentes de ciberseguridad que se presenten, configurando un ciberespacio estable y resiliente.

4 Estado actual de la ciberseguridad: normas, instituciones, panorama de riesgos

A. Normas e instituciones

La institucionalidad vigente en materia de ciberseguridad se encuentra distribuida en diversos organismos y entidades. Esto hace necesario la coordinación estratégica de los distintos esfuerzos, de sus roles y funciones, y el establecimiento de prácticas y criterios técnicos comunes, con el objetivo de mejorar la eficiencia y eficacia en el ámbito de la ciberseguridad.[4]

En esta materia, nuestro país cuenta con un conjunto de normas legales y reglamentarias que se hacen cargo directa e indirectamente del fenómeno de la ciberseguridad que resulta necesario revisar y actualizar conforme a las directrices que plantea esta política y a los compromisos internacionales de Chile, por ejemplo, la ley Nº 19.223 sobre delitos informáticos o la ley Nº 19.628 sobre protección de la vida privada, entre otras.

B. Panorama de riesgos

Atendido el carácter global del ciberespacio, los riesgos y amenazas provienen de Chile y del exterior, y se originan tanto en causas naturales como en actividades delictuales, por ejemplo, en labores de espionaje y vigilancia llevadas a cabo con diversos fines, afectando la confidencialidad, integridad y disponibilidad de los activos de información en el ciberespacio, y con ello, los derechos de las personas.[5]

A nivel global, existen abundantes antecedentes sobre ciberataques y actividades de espionaje en la red. La interceptación masiva de redes de telecomunicaciones, la inutilización del servicio de internet, el espionaje contra gobiernos y empresas, además de ataques contra infraestructuras críticas como servicios básicos, instituciones financieras y entidades gubernamentales, han marcado la pauta informativa a nivel global en esta materia.

A nivel regional, en el año 2013 los países que registraron el mayor número de ciberataques en Latinoamérica fueron Brasil, Argentina, Colombia, México y Chile. Los accesos o robo de información desde computadores o dispositivos infectados predominaron en la región[6].

Asimismo, los ciberdelitos cometidos en Chile confirman el carácter transnacional de éstos, especialmente los relacionados con el uso fraudulento de tarjetas de crédito y débito, estafas informáticas, entre otros.

La política considera esta clase de amenazas, especialmente respecto a aquellas que afecten las infraestructuras críticas del país.

---

4 Ver anexo Nº1 con detalle de la normativa e institucionalidad existente en materia de ciberseguridad.

5 Ver anexo Nº2 con información sobre riesgos para el país en el ciberespacio.

6 Prandini, P. y Maggiore, M. 2013. Ciberdelito en América Latina y El Caribe. Una visión desde la sociedad civil. Proyecto Amparo, Sección de Estudios. LACNIC Registro de Direcciones de Internet para América Latina y Caribe. pp. 3.

5 Hoja de ruta de la política

La presente política de ciberseguridad tiene dos componentes centrales: una política de Estado, diseñada con objetivos orientados al año 2022, y una agenda de medidas específicas, que serán implementadas entre los años 2017 y 2018.

El objetivo de este diseño es proponer una visión general de hacia dónde debe moverse el país en el mediano y largo plazo, junto con un set de medidas que puedan ser implementadas y evaluadas en lo que resta de gobierno, dejando a la siguiente administración la tarea de revisar la política y plantear una agenda que pueda abarcar el siguiente gobierno.

A. Objetivos de política para el año 2022

En esta política se plantean objetivos de alto nivel con una mirada de largo plazo, que permita orientar los esfuerzos del país hacia la consecución de dichas metas, sirviendo a la vez de guía para priorizar y racionalizar las medidas contenidas en el presente documento.

Junto con lo anterior, la política contiene una serie de funciones mínimas imprescindibles y el correspondiente diseño institucional que deberá hacerse cargo de éstas, tanto en el corto plazo, como en el mediano y largo plazo (2017-2022).

B. Agenda de medidas 2017-2018 y evaluación

Desarrollando los objetivos de la política, se propone una agenda a implementar durante el bienio 2017-2018, que permitirá poner en marcha un esfuerzo conjunto de parte del gobierno y el sector privado en materia de ciberseguridad, orientada a la adopción de las medidas priorizadas y a la preparación de diversos insumos que permitan revisar y ampliar la política a fines del año 2017.

C. Políticas integradas complementarias en materia digital

La presente política de ciberseguridad se enmarca en un conjunto de políticas que el Gobierno ha implementado o se encuentra desarrollando en materia digital, con el objeto de contar con definiciones claras y sistémicas sobre el ciberespacio:

> Agenda Digital 2020

La Agenda Digital 2020[7] es una hoja de ruta para avanzar hacia el desarrollo digital del país, mediante la definición de objetivos de mediano plazo, líneas de acción y medidas concretas. Fue lanzada el segundo semestre del año 2015, y aspira a que el uso masivo de las tecnologías se transforme en un medio para reducir las desigualdades, permitiendo abrir más y mejores oportunidades de desarrollo, y contribuir al respeto de los derechos de todos los chilenos y chilenas.

En la Agenda existe una medida específica (Nº25) que apunta a la elaboración de una estrategia de ciberseguridad, que la presente política viene a cumplir. Además, varias medidas de la Agenda

7 Disponible en: http://www.agendadigital.gob.cl/

potencian y complementan la presente política, destacando el impulso que se entrega a una nueva Ley de Protección de datos personales, el resguardo a los derechos de los consumidores en internet, el desarrollo de un Plan Nacional de Infraestructura de Telecomunicaciones, el perfeccionamiento de la normativa sobre firma electrónica, entre otras.

> Política nacional de ciberdefensa

Dado que las redes y sistemas de información de la Defensa Nacional constituyen una infraestructura crítica para la seguridad exterior y el ejercicio de la soberanía del país, y a las atribuciones constitucionales y legales de la Defensa Nacional, el Ministerio de Defensa, durante el año 2017 preparará y publicará políticas específicas de ciberdefensa, que contemplen las definiciones políticas en torno a cómo serán protegidas estas redes, y cómo las capacidades de la Defensa Nacional pueden colaborar en la formación de un ciberespacio libre, abierto, seguro y resiliente para el país.

> Política internacional para el ciberespacio

Uno de los objetivos de alto nivel de la presente política dice relación con la cooperación y relaciones internacionales en torno a la ciberseguridad en el contexto global. Sin embargo, es imprescindible que el país integre estos objetivos con otros tales como el desarrollo, los derechos humanos, la defensa y otros relacionados, para consolidarlos e integrarlos en la política exterior de Chile.

Para ello, la presente política contempla una medida específica vinculada con la elaboración de una estrategia en estas materias por parte del Ministerio de Relaciones Exteriores, lo que a su vez es consistente y pone en marcha la medida Nº11 de la Agenda Digital 2020, que apunta a generar una visión país sobre gobernanza de internet.

6 Objetivos de política para el año 2022

A. 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

> 1. Concepto. Identificación y gestión de riesgos

La ciberseguridad es una condición caracterizada por un mínimo de riesgos para el ciberespacio, entendido como el conjunto de infraestructuras físicas, lógicas y las interacciones humanas que allí ocurren. En este conjunto, y siguiendo estándares internacionales, los atributos claves a proteger son la confidencialidad, integridad y disponibilidad de la información, los que a su vez generan un ciberespacio robusto y resiliente.

Dentro de este marco no se considera la ampliación de capacidades de vigilancia estatal o privada utilizando tecnologías digitales, las que obedecen a objetivos de orden público o seguridad nacional que son discutidas en otras instancias, y con una lógica diferente a la aquí expuesta. Las medidas de monitoreo que aquí se consideran servirán únicamente al objetivo de gestionar los riesgos para la seguridad de la información en el ciberespacio.

A partir de la Política, se crearán modelos de prevención y gestión de riesgos del ciberespacio, o riesgos físicos que le afecten, actualizados regularmente bajo un modelo de mejora continua, que servirán de base a las medidas técnicas que deben adoptarse para prevenir, gestionar y superar los riesgos cuando estos se verifican, con énfasis en la resiliencia y continuidad de servicios dentro de un marco temporal acotado, con la finalidad de maximizar los niveles de ciberseguridad del país.

> 2. Protección de la infraestructura de la información

La infraestructura de la información la conforman las personas, procesos, procedimientos, herramientas, instalaciones y tecnologías que soportan la creación, uso, transporte, almacenamiento y destrucción de la información.

Dentro de las infraestructuras de la información, existe un conjunto especialmente relevante para la marcha del país, las denominadas infraestructuras críticas de la información (ICI), que comprende las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado.

Se pondrá particular atención al impacto que pueda tener un incidente de seguridad de la información en infraestructuras físicas controladas o monitoreadas desde el ciberespacio, y en la seguridad de los sensores y dispositivos de control industrial que habilitan dichas acciones.

Las ICI se deberán diseñar con una arquitectura que maximice su robustez y resiliencia frente a eventos que las puedan inhabilitar, adaptándose a fenómenos de la naturaleza, intervenciones humanas o interferencias informáticas tales como incidentes involuntarios o ciberataques.

3. Identificación y jerarquización de las infraestructuras críticas de la información

Los sectores que componen la clasificación de ICI son muy similares y se repiten en varias clasificaciones a nivel internacional. En el caso chileno, mientras se adopta una política específica para infraestructuras críticas, la infraestructura de la información de los siguientes sectores será considerada como crítica: **energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa**, entre otras.

La política de infraestructuras críticas contendrá un esquema acabado de áreas, funciones y entidades estatales responsables que servirán para identificar y delimitar el nivel de criticidad de cada sector.

Los órganos técnicos encargados de ejecutar medidas que se deriven de la presente política, deberán considerar estándares especiales de ciberseguridad, atendido sus particulares niveles de madurez, para las ICI, especialmente respecto a sus procesos esenciales.

En el mediano plazo se avanzará en la implementación de medidas que garanticen la continuidad de servicio mediante redundancia de instalaciones físicas de algunas ICI, especialmente en los sectores de telecomunicaciones, administración pública, protección civil y defensa.

4. Contar con equipos de respuesta a incidentes de ciberseguridad

Siguiendo las mejores prácticas internacionales, es imprescindible contar con una estructura de prevención, monitoreo, gestión y respuesta a incidentes de seguridad de la información a nivel nacional.

Los órganos base de esta estructura son los *Computer Security Incident Response Team,* (CSIRT), o equipos de respuesta a incidentes de seguridad informática. Hoy en Chile estos centros requieren de recursos humanos y financieros, un marco institucional claro y mecanismos para operar de manera coordinada entre sí, de manera de incentivar su creación y operación en diversos sectores de la vida nacional.

Chile contará con un CSIRT nacional que recopile y sistematice información proveniente de otros CSIRT (nacionales y extranjeros), promoverá la coordinación de acciones entre CSIRT sectoriales y tendrá la autoridad necesaria para coordinar la respuesta técnica frente a incidentes que comprometan la seguridad del país.

Se reforzará el actual CSIRT de Gobierno y se creará uno específico para la Defensa Nacional. Por otra parte, deberá evaluarse la pertinencia de crear un CSIRT de infraestructuras críticas.

Se promoverá la creación de CSIRT sectoriales, por diversos actores públicos, privados, académicos y de la sociedad civil.

5. Implementación de mecanismos estandarizados de reporte, gestión y recuperación de incidentes

Existirán mecanismos que permitan el reporte centralizado y estandarizado de incidentes de ciberseguridad, de manera de contar con un panorama amplio y en tiempo real de los incidentes que se vayan generando en el país.

Estos mecanismos serán obligatorios para el gobierno central y ciertos sectores regulados, y voluntarios, en principio, para los otros actores que quieran sumarse. La cantidad de información requerida se limitará a la estrictamente necesaria para caracterizar y poder gestionar el tipo de amenaza, evitando especialmente la recolección y procesamiento que afecten la privacidad de las personas.

Para tal efecto, el CSIRT Nacional mantendrá una plataforma segura y confidencial de colaboración en materia de incidentes de ciberseguridad, con el objeto de agregar la información pertinente y, en conjunto con otros órganos públicos y privados, establecerá una red de trabajo.

Al mismo tiempo, los organismos públicos y las ICI contarán con instancias institucionales encargadas de la seguridad de la información, junto con planes de gestión y recuperación de incidentes, con énfasis en mantener la continuidad de sus operaciones y minimizar los daños producidos por los incidentes verificados.

Sumado a lo anterior, se promoverá el reporte de vulnerabilidades informáticas por parte de usuarios y expertos en el área, mediante la adopción de marcos de entrega responsable de información, modelos de recompensas por la detección de problemas de seguridad, y otros mecanismos que incentiven la revelación responsable.

> 6. Exigencia de estándares diferenciados en materia de ciberseguridad

Todas las infraestructuras de la información que dependan o que provean productos o servicios al Gobierno de Chile o servicios a la ciudadanía, deberán contar con un nivel básico de adopción de medidas de ciberseguridad de acuerdo a estándares que contemplen la confidencialidad, integridad y disponibilidad de la información y de los sistemas que operan, acorde a los riesgos y amenazas que enfrenten, de manera consistente con su tamaño, madurez, y el nivel de criticidad y confidencialidad de la información y/o procesamientos que soportan.

En el caso de las infraestructuras críticas de la información, deberán evaluar sus riesgos y enfrentarlos de acuerdo a estándares que contemplen la confidencialidad, integridad y disponibilidad de la ICI, para contar con un sistema efectivo y armónico de seguridad que permita la prevención, manejo y recuperación de ciberataques y otros incidentes de seguridad informática, contando con planes de contingencia para asegurar la continuidad operativa de sus servicios.

Los estándares y mejores prácticas a emplear serán compatibles con los esfuerzos internacionales, asegurando la confidencialidad, integridad y disponibilidad de la información, sin prescribir soluciones específicas, salvo casos calificados.

B. El Estado velará por los derechos de las personas en el ciberespacio

> 1. Prevención de ilícitos y generación de confianza en el ciberespacio

La prevención, la disuasión, el control y la sanción de los ilícitos son indispensables para minimizar los riesgos y amenazas en el ciberespacio, de manera de contribuir a la generación de confianza en las actividades que en él se desarrollan.

Existen múltiples actividades ilícitas que se llevan a cabo en el ciberespacio, como la sustracción de información estratégica, la interrupción de sistemas de servicios en línea, fenómenos como el secuestro de información *(ransomware), phishing, pharming* y el uso fraudulento de tarjetas de crédito o débito, entre otras modalidades.

A nivel global, existen antecedentes sobre ciberataques consistentes en actividades de espionaje y ataques de denegación distribuida de servicio (DDoS) en internet, la interceptación masiva de redes de telecomunicaciones, ataques contra infraestructuras críticas como bancos, servicios básicos e instituciones gubernamentales, por mencionar algunos. Esta política procurará minimizar los riesgos asociados a estas amenazas.

Junto con políticas públicas que se hagan cargo de prevenir y sancionar ilícitos, también es posible generar confianza en el ciberespacio mediante el empleo de las mismas tecnologías. En ese sentido, se promoverá la adopción de soluciones técnicas que permitan aumentar la seguridad de los usuarios del ciberespacio, especialmente aquellas que colaboren con la gestión de la identidad en este ambiente, como la adopción masiva de certificados digitales (firma digital) en sitios web y por parte de las personas y organizaciones, como una manera de asegurar las comunicaciones e identidad de los usuarios.

Junto con lo anterior, esta política reconoce el valor de las tecnologías de cifrado, que permiten dotar de niveles de confidencialidad e integridad de la información sin precedentes en nuestra historia. Las medidas basadas en esta política deberán promover la adopción de cifrado punto a punto para los usuarios, en línea con los estándares internacionales; y en ningún caso se promoverá el uso intencional de tecnologías poco seguras, ni la obligación a ninguna persona u organización que provea servicios digitales, de implementar mecanismos de "puerta trasera" que comprometan o eleven los riesgos asociados a las tecnologías de seguridad empleadas.

> 2. Establecimiento de prioridades en la implementación de medidas sancionatorias

A diferencia de los ilícitos que se cometen en el espacio físico, en el ciberespacio existen algunas dificultades para la persecución y sanción de estos delitos. Entre otros, destacan la identificación de los autores, el tiempo que pasa entre la ejecución del ilícito y la reacción de la víctima, las bajas tasas de denuncia y la escasa posibilidad de perseguir a los infractores, pues los organismos persecutores operan en los límites territoriales del Estado mientras el ciberespacio es esencialmente un lugar sin fronteras.

Las medidas sancionatorias deben implementarse teniendo en cuenta ese contexto, de manera complementaria con esta política.

La actualización de nuestra legislación, impulsada por la decisión de adherir a la Convención sobre Ciberdelitos del Consejo de Europa[8], la mejora y fortalecimiento de la normativa actual y la creación de medidas transversales en lugar de sectoriales, constituyen importantes objetivos en este ámbito.

> 3. Prevención multisectorial

Dado que los ciberataques y ciberdelitos pueden ser llevados a cabo por organismos estatales, grupos organizados o personas individuales y que las amenazas provienen tanto del interior como del exterior del país, la respuesta debe ser multisectorial, involucrando tanto al sector privado, la academia, la sociedad civil y por supuesto a los organismos de persecución penal, de defensa y las víctimas.

Para ello, es primordial generar instancias apropiadas de coordinación, encuentro y colaboración y fortalecer significativamente las capacidades técnicas y el acceso a capacitación de los fiscales y

8 Disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

jueces, las capacidades periciales y forenses de las policías y generar pautas de cuidado mínimas para toda la población.

Se deben definir capacidades de levantamiento, estandarización e integración de datos e información relacionados con el cibercrimen, aumentar la capacidad para investigar y generar evidencia respecto al mismo.

> 4. Respeto y promoción de derechos fundamentales

Todas las medidas propuestas por la política se deben diseñar y ejecutar con un enfoque de derechos fundamentales, atendido su carácter universal e indivisible y sobre la base que el ciberespacio es un ambiente donde las personas cuentan con los mismos derechos que en el mundo físico[9]. Así, la política considera y promueve:

- La característica de bien público global de internet, que implica que no se puede privar a los usuarios de acceso a la red sino por razones de fuerza mayor debidamente justificadas, y nunca por razones difusas como el orden público, la seguridad nacional, o la honra u honor de algún individuo, sin importar su calidad o investidura.
- En razón de lo mismo, y en atención a la disponibilidad de la información como atributo esencial de la ciberseguridad, esta política apoyará los esfuerzos públicos y privados en materia de acceso a la información y la cultura de la población a través de medios digitales.
- Junto con lo anterior, se incluye el respeto al principio de neutralidad de la red, de modo tal que los proveedores de servicios de internet no puedan discriminar ni limitar el acceso a contenidos arbitrariamente, salvo justificación legal.
- Esta política también respeta y promueve el respeto a la libertad de expresión, considerando dentro de esta protección no sólo a los medios de comunicación, sino también a la generalidad de la población, y a los intermediarios que permiten comunicar estos mensajes, como las redes sociales.[10] Cualquier injerencia en este derecho deberá ser llevada a cabo de acuerdo con los estándares nacionales e internacionales de Derechos Humanos en la materia.
- La protección de la vida privada y la inviolabilidad de las comunicaciones de los usuarios en el ciberespacio, incluyendo protecciones contra la recolección, procesamiento y publicación no autorizada de sus datos personales; la transparencia en el manejo de esos datos por actores privados y públicos; y como fue mencionado, la protección de tecnologías esenciales para ofrecer seguridad y confianza en el ciberespacio a sus usuarios.
- La protección del debido proceso en relación con las medidas que afecten la seguridad de la información, procurando que las medidas de vigilancia y persecución penal en el ciberespacio cumplan con estándares internacionales de protección como los principios de idoneidad, necesidad y proporcionalidad.[11] Estas medidas no sólo serán aplicables a la persecución penal

9 En ese sentido, la resolución A/HRC/20/L.13 del Consejo de Derechos Humanos de las Naciones Unidas declaró que "los derechos de las personas también deben estar protegidos en Internet".

10 El rol de los intermediarios de internet ha ganado una creciente atención, por su rol crítico en asegurar derechos como el de Libertad de Expresión. Al respecto, pueden consultarse marcos de referencia como los principios de Manila. [en línea] Disponibles en https://www.manilaprinciples.org/es

11 En ese sentido, una herramienta útil de análisis es el documento "Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones". [en línea] Disponible en https://es.necessaryandproportionate.org/text

del Estado, sino al actuar de todos sus órganos, velando también la aplicación de este derecho entre usuarios del ciberespacio. La vigilancia masiva e indiscriminada en el ciberespacio, atenta gravemente contra los derechos fundamentales.

En los esfuerzos en materia de derechos fundamentales se considerarán especialmente los derechos de grupos vulnerables, como los niños, niñas y adolescentes, personas de la tercera edad, personas con discapacidad y minorías étnicas, entre otras; además del empleo de un enfoque de género, que permita hacer visibles y enfrentar las desigualdades que enfrentan los diversos usuarios del ciberespacio.

La política procurará que todas las personas puedan disfrutar de un ciberespacio seguro y libre de abusos tales como el acoso en línea, el robo de información personal, la vigilancia masiva, y otras prácticas que perjudican especialmente a sectores menos privilegiados de la sociedad. En particular, se llevarán adelante esfuerzos a todo nivel para que la ciberseguridad no sea considerada un lujo para las personas ni para las organizaciones del país.

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

> 1. Una cultura de la ciberseguridad

Las TIC contribuyen a la formación equitativa e inclusiva del acervo cultural, tecnológico y económico del país y al desarrollo integral de las personas.

Por ello, se fomentará a todo nivel, la creación de una cultura de la ciberseguridad con el objeto que la sociedad cuente con las herramientas y el conocimiento para entender este ámbito de relaciones humanas, con sus ventajas, oportunidades y riesgos, y pueda manejarlos adecuadamente.

> 2. Sensibilización e información a la comunidad

Se sensibilizará a las personas sobre los riesgos y amenazas del ciberespacio para lograr un uso seguro de las plataformas que prestan servicios a la comunidad tanto desde las instituciones públicas como de agentes privados.

Se informará a la comunidad sobre el buen uso, las medidas de cuidado personal y seguridad en el ciberespacio.

> 3. Formación para la ciberseguridad

Esta necesidad depara grandes desafíos a nuestro sistema educacional. La formación temprana y avanzada de la población no está ajena a estos desafíos y corresponde hacerse cargo de las brechas digitales producto de desigualdades en recursos, capacidades, infraestructura, conectividad, entre otras.

Para esto es crucial apoyar la implementación de iniciativas que fomenten y desarrollen una cultura digital **consciente, competente, informada y responsable** que incluya a todos los actores relevantes entendiendo que estamos frente a un esfuerzo colectivo en pos de un beneficio común y de largo plazo.

D. El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales

1. Principios de política exterior chilena

La política exterior de Chile tiene como base una serie de principios que orientan su diplomacia y su acción: el respeto al derecho internacional, la promoción de la democracia, el respeto a los derechos humanos, la prevención de conflictos, la solución pacífica de las controversias y la responsabilidad de cooperar en el ámbito internacional, los cuales guían los intereses de nuestra política exterior, a saber: la contribución al fortalecimiento del multilateralismo y la promoción de la paz y la seguridad internacional, entre otros[12].

La emergencia del ciberespacio, y muy especialmente internet, como un bien público global, nos obliga a enfrentar el desafío de gestionar sus riesgos a todo nivel, donde el plano internacional reviste particular importancia, considerando el carácter global y transfronterizo del mismo.

La ciberseguridad es un concepto transversal y multifactorial, que en el plano internacional significa tanto la posibilidad de construir capacidades, enfoques y medidas comunes en cooperación y asistencia con otros países, como la convicción de que un trabajo diplomático sostenido en el ámbito multilateral y de múltiples partes interesadas permite disminuir los riesgos de conflicto en el ciberespacio.

Para lograr lo anterior, el Ministerio de Relaciones Exteriores deberá coordinar con el resto de los ministerios y agencias de gobierno, la política internacional en materia de ciberseguridad.

2. Cooperación y asistencia

En materia de cooperación internacional dentro del ámbito bilateral, se potenciará la relación con otros países en ciberseguridad, bajo diversas modalidades como la asistencia desde o hacia Chile, el intercambio de información y experiencias, la implementación y profundización de mecanismos de diálogo político en la materia, y el empuje de medidas de transparencia y construcción de confianza en el ciberespacio, priorizando una aproximación multiagencial a los temas.

3. Reforzar la participación en instancias multilaterales y en instancias de múltiples partes interesadas (*multistakeholder*)

Se deben orientar los esfuerzos para promover que el campo digital sea un entorno libre, abierto y seguro para todos los usuarios del ciberespacio.

Es necesario fortalecer el trabajo del país en la materia, tomando en consideración los especiales desafíos que se plantean, tanto en sus condiciones técnicas, en el carácter global y descentralizado de la red, como en sus dimensiones políticas, caracterizadas por un sistema de gobernanza de internet de múltiples partes interesadas, donde el sector privado y la sociedad civil tienen un especial rol.

Dentro de ese marco, se incrementará la 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, involucrando activamente a las diversas partes interesadas en el debate.

12 Más información en:http://www.minrel.gov.cl/minrel/site/artic/20080802/pags/20080802194424.html

4. Fomentar normas internacionales que promuevan la confianza y seguridad en el ciberespacio

Aun cuando prácticamente no existen instrumentos normativos específicos, el ciberespacio está regulado tanto por las leyes nacionales como por la normativa internacional general aplicable, por lo que el desafío consiste principalmente en identificar e interpretar las normas relevantes del derecho internacional aplicables.

No obstante, existen desafíos que deben enfrentarse mediante acuerdos y normas internacionales específicas, como la Convención sobre Ciberdelitos a la que el país adherirá, efectuando reservas y prevenciones consistentes con la presente política.

Simultáneamente se promoverá el debate y la adopción de acuerdos multilaterales y bilaterales que fomenten la cooperación y asistencia mutua en ciberseguridad, tanto a nivel de instrumentos formales como de acuerdos y arreglos informales que apunten a la transparencia y construcción de confianzas internacionales en la materia.

E. El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos

1. Importancia de la innovación y desarrollo en materia de ciberseguridad

Las actividades de seguridad interior y defensa exterior en general requieren de un fuerte componente de innovación y desarrollo, que redundan en un mayor desarrollo de la industria nacional en el área. En ese marco, el sector de la ciberseguridad requiere de un especial esfuerzo, atendida su relativa novedad e importancia estratégica para el país en su conjunto.

2. Ciberseguridad como medio para contribuir al desarrollo digital de Chile

Mientras el tamaño del sector TIC representa cerca de un 3~4,12% del total de la economía chilena, en los países OECD este sector promedia un 6% de participación en la economía de los países[13], generando una brecha entre ambas realidades que Chile subsanará, en parte, mediante el desarrollo del componente de ciberseguridad dentro de esa industria.

Se generará tanto una mayor demanda a la industria de tecnologías de la información como un mayor desarrollo industrial en la materia que permita al país acercarse a los indicadores de la OECD, junto con potenciar los objetivos de la política.

3. Desarrollo de la industria de ciberseguridad en Chile

No existen cifras específicas respecto al nivel de desarrollo de la industria nacional, sólo estudios que exploran esta alternativa[14]. Los esfuerzos por desarrollar una industria de ciberseguridad en el país

13 Existen actualmente estudios que dan una aproximación al valor del PIB que aporta el sector TIC, como por ejemplo, el "Índice País Digital" realizado por la Fundación País Digital en alianza con la UDD, entregado en enero del año 2015, estimó que el tamaño del sector TIC representa un 3% sobre el total de la economía chilena (fuente año 2012). Por otra parte, la Subsecretaría de Economía encargó a F&K Consultores el "Estado del desarrollo digital en Chile", en marzo de 2015, el cual entregó que el valor agregado del sector TIC llega a un 4,12% respecto al valor agregado total (fuente año 2011).

14 Informe "Tecnologías de la Información y Comunicación en Chile: Áreas de investigación y capacidades, informe de estado del arte", Conicyt, 2010. "Índice País Digital", Fundación País Digital en alianza con la UDD, enero de 2015. "Estado del desarrollo digital en Chile", F&K Consultores, marzo de 2015.

irán acompañados de estudios que caractericen la industria e identifiquen dominios estratégicos para desarrollar en el corto, mediano y largo plazo.

En particular, un dominio que normalmente se desarrolla en la experiencia comparada, es la industria nacional vinculada al desarrollo y uso de estándares de cifrado, atendida su importancia estratégica para la seguridad exterior del país.

> 4. Contribuir a la generación de oferta por parte de la industria local

Se adoptarán medidas que ayuden a crear y fortalecer una industria nacional de servicios, tecnologías y gestión de la ciberseguridad, a través programas e iniciativas que apunten a la producción de nuevos bienes y servicios en el área. Para ello, se creará un polo de desarrollo en el área, en línea con la Agenda de Productividad, Innovación y Crecimiento[15] y la Agenda Digital 2020.

> 5. Generación de demanda de parte del sector público basado en los intereses estratégicos del Estado

A partir de la generación de demanda del sector público en base a sus necesidades, intereses estratégicos y de seguridad, se promoverá el fortalecimiento de una industria nacional de servicios, tecnologías y gestión de la ciberseguridad, alineada con estándares técnicos internacionales.

15 Disponible en: http://www.agendaproductividad.cl/

7 Funciones e institucionalidad necesarias para desarrollar una política nacional de ciberseguridad

A. Institucionalidad para la ciberseguridad

Para cumplir con esta ambiciosa política nacional de ciberseguridad y siguiendo el ejemplo de diversos países que han iniciado este proceso hace algunos años, resulta imprescindible para Chile contar con un modelo de gobernanza de la ciberseguridad que se haga cargo de, al menos, desempeñar las funciones que se identifican como esenciales, y que no están siendo abordadas o se ejecutan de manera descoordinada en el país, por lo cual se propone la creación de una institucionalidad que asuma dichas funciones.

El modelo de gobernanza y la estructura organizacional moderna, acorde a las necesidades del ciberespacio y el desarrollo digital del país, será materia de ley a ser preparada y presentada por los actores institucionales responsables de esta materia. Asimismo, se evaluará la creación de un consejo consultivo asesor, de integración multisectorial.

Las funciones que se identifican como esenciales son la gestión de relaciones interinstitucionales, gestión de incidentes, funcionamiento como punto de contacto nacional e internacional en este ámbito, función comunicacional, función normativa técnica y asesora en normativa general, función de seguimiento y evaluación de medidas.

Para lo anterior, se considerará especialmente la correspondencia de la institucionalidad de ciberseguridad con las iniciativas complementarias que se están desarrollando en materia de gobernanza digital en la administración del Estado.

B. Gobernanza transitoria en ciberseguridad

Mientras se discute y aprueba en el Congreso Nacional el proyecto de ley sobre ciberseguridad, que contendrá la propuesta de institucionalidad definitiva, ciertas funciones identificadas como esenciales, deberán ser ejercidas temporalmente por algunas de las instituciones que forman parte de la actual estructura de Gobierno, por ejemplo, en materia técnica para la gestión de los incidentes que se generen en la Red de Conectividad del Estado cumplirá tal rol el CSIRT Gob, mientras que a nivel político, se propone prorrogar la existencia y ampliar el mandato del Comité Interministerial sobre Ciberseguridad, respecto de la función comunicacional, de coordinación y seguimiento de medidas presentadas en la PNCS.

8 Medidas de política pública 2017-2018

Las presentes medidas forman parte de la agenda de políticas públicas a implementar, basadas en los objetivos estratégicos expuestos anteriormente[16].

	MEDIDA	RESPONSABLE/ COLABORADORES	OBJETIVOS PNCS
1	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.	MISP - MINDEF - MINHACIENDA (CICS supervisor de la medida)	A
2	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.	MINSEGPRES	A
3	Añadir una dimensión de ciberseguridad a la preparación y gestión de contratos de concesión de obra pública.	MOP (Dirección de concesiones)	A
4	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.	MISP	A
5	Creación de una norma técnica para el desarrollo o contratación de software en el Estado, acorde a estándares de desarrollo seguro.	MINSEGPRES	A
6	Creación de una plataforma para agregar información sobre incidentes de ciberseguridad.	CSIRT	A
7	Decretar coordinadamente requisitos actualizados de seguridad para sectores económicos regulados.	MTT - Superintendencias - CSIRT	A
8	Identificar un set mínimo de riesgos para las infraestructuras críticas de la información.	CSIRT	A

16 El primer organismo es el responsable principal de la tarea, y los organismos sucesivos colaboran en su ejecución.

La denominación de CSIRT corresponde al actual equipo de seguridad de la Red de Conectividad del Estado, que asumirá progresivamente funciones operativas identificadas en la presente política.

Las instituciones públicas están identificadas con las siguientes siglas: CICS, Comité Interministerial sobre Ciberseguridad; MISP, Ministerio del Interior y Seguridad Pública; MTT, Ministerio de Transportes y Telecomunicaciones; MINDEF, Ministerio de Defensa Nacional; MINHACIENDA, Ministerio de Hacienda; ANI, Agencia Nacional de Inteligencia; MINJUSTICIA, Ministerio de Justicia y Derechos Humanos; MINSEGPRES, Ministerio Secretaría General de la Presidencia; MOP, Ministerio de Obras Públicas; MINEDUC, Ministerio de Educación; MINREL, Ministerio de Relaciones Exteriores; MSGG, Ministerio Secretaría General de Gobierno; MINECON, Ministerio de Economía, Fomento y Turismo.

Cuando se denomina un ministerio sin identificar un servicio público o subsecretaría específica, se refiere a la subsecretaría que forma parte del Comité Interministerial sobre Ciberseguridad o, en caso que el Ministerio correspondiente no forme parte del Comité, a una tarea que debe emprender el Ministerio correspondiente de manera global.

	MEDIDA	RESPONSABLE/ COLABORADORES	OBJETIVOS PNCS
9	Implementar una matriz estandarizada para reportes de incidencias en materia de ciberseguridad.	CSIRT, MINSEGPRES	A
10	Incorporar la dimensión de ciberseguridad en el sistema nacional de emergencias.	MISP (CICS supervisor de la medida)	A
11	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.	MISP - MINDEF - ANI- MINREL- MINSEGPRES	A
12	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.	MTT	A
13	Actualizar normativa sobre delitos informáticos	MISP - MINJUSTICIA	B
14	Diseñar e implementar una matriz estandarizada de denuncias de ciberdelitos.	MISP (con policías y ANI) - MINJUSTICIA	B
15	Promover el fortalecimiento de las capacidades de investigación y análisis forense relacionadas con el ciberdelito.	MISP (con ANI y policías)	B
16	Generar primer punto de difusión de información para el ciudadano sobre Ciberseguridad, basado en los diferentes canales electrónicos y redes sociales que ofrece internet.	MISP - MSGG (CICS supervisor de la medida)	C
17	Instaurar el mes de la Ciberseguridad en octubre de cada año, promoviendo y consolidando actividades de sensibilización en todos los niveles. Además, de en Febrero participar en el día internet segura.	MISP - MSGG (CICS supervisor de la medida)	C
18	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.	MSGG (CICS supervisor de la medida)	C
19	Generar guías de buenas prácticas para la ciudadanía y el sector público.	CICS	C
20	Conformar una mesa intersectorial para fomentar la formación en ciberseguridad en todos los niveles y estamentos del sector educativo.	MINEDUC- MINECON (Mesa Capital Humano) (CICS supervisor de la medida)	C

	MEDIDA	RESPONSABLE/ COLABORADORES	OBJETIVOS PNCS
21	Diseñar e implementar una campaña de ciberseguridad orientada a los adultos mayores, que considere medidas de capacitación y difusión.	MDS (Senama) - MINECON (Mesa Capital Humano) (CICS supervisor de la medida)	C
22	Incorporación de Seguridad en Internet en programas específicos de MINEDUC, reforzando la iniciativa ENLACES.	MINEDUC (Enlaces) - MINECON(Mesa Capital Humano) (CICS supervisor de la medida)	C
23	Apoyar decididamente el establecimiento a nivel internacional de procesos de consultas políticas regionales, subregionales y multilaterales, con especial énfasis en la región.	MINREL	D
24	Avanzar en el establecimiento de mecanismos bilaterales de trabajo, diseñando agendas e implementando instancias de consultas políticas transversales con países afines.	MINREL	D
25	Elaborar un documento de política internacional de Chile sobre el ciberespacio y ciberseguridad.	MINREL (CICS supervisor de la medida)	D
26	Establecimiento de un grupo de trabajo interagencial para abordar temas internacionales relativos al ciberespacio.	MINREL - OTROS	D
27	Propiciar el intercambio de experiencias con otros países en materia de ciberseguridad, con énfasis en la implementación y evaluación de estrategias y políticas.	MINREL	D
28	Analizar la regulación y aplicación del régimen vigente de compras públicas respecto a apoyo productivo e intereses nacionales estratégicos.	MINHACIENDA (Dirección Chilecompra) - MISP - MINDEF	E
29	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.	CORFO - MINDEF - MINECON	E
30	Estudio de incentivos tributarios, subsidios o mecanismos de I+D+i para desarrollo y adopción de estándares de ciberseguridad.	MINHACIENDA - MINECON - CORFO	E
31	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.	MINHACIENDA- MINECON	A, B

	MEDIDA	RESPONSABLE/ COLABORADORES	OBJETIVOS PNCS
32	Establecer una o más instancias de colaboración multisectoriales con diversos actores sociales (ONG, empresas, gremios, academia y otras)	CICS (coordinador de mesas)	A, B, C
33	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.	MISP	A, C
34	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.	CSIRT	A, C
35	Incorporar estándares de ciberseguridad a los proveedores del Estado, exigiendo requisitos específicos para proveedores TIC, y analizando otros para el resto de los proveedores.	MINHACIENDA (Dirección Chilecompra)	A, E
36	Incorporar en la Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC) un set de preguntas vinculadas a los ciberdelitos.	MISP (Subsecretaría de Prevención del Delito)	B, C
37	Generar, y actualizar regularmente, catastro de oferta en capacitación para funcionarios públicos, sobre ciberseguridad disponible en organismos internacionales e instituciones nacionales.	MISP - MINREL	B, C, D
38	Adherir e implementar la Convención sobre Ciberdelitos del Consejo de Europa.	MISP - MINREL - MINJUSTICIA- MINISTERIO PÚBLICO	B, D
39	Fomentar el patrocinio del Estado a proyectos de I+D+i con financiamiento público o privado, nacional o internacional en materias de Ciberseguridad.	CICS	C, E
40	Promover el desarrollo de capital humano avanzado en asuntos de Ciberseguridad en los distintos ámbitos técnico-profesionales.	CORFO - MINECON (Mesa Capital Humano) Actores del mundo público, privado y académico	C, E
41	Apoyar la exportación de productos y servicios nacionales en el área de ciberseguridad, identificando ferias internacionales y evaluando posibilidades de apoyo.	MINREL (Prochile) - MINECON	D, E

9 Anexos

Anexo Nº1: Normas e instituciones que intervienen en ciberseguridad en Chile

1. NORMAS RELEVANTES A NIVEL NACIONAL

a. Constitución Política de la República

- **Artículo 8º,** relativo a la transparencia pública.
- **Artículo 19º,** que contempla un catálogo de derechos fundamentales donde son especialmente relevantes: Nº2, igualdad ante la ley; **Nº3 y 7**, relativos al debido proceso y seguridad individual; **Nº4 y 5**, sobre protección de la vida privada e inviolabilidad de las comunicaciones; **Nº12**, que garantiza la libertad de expresión y de información; y **Nº24 y 25**, relativos a la propiedad y libertad de creación.
- **Artículo 24º,** que otorga a quien ejerza la Presidencia de la República la autoridad para conservar el orden público en el interior y la seguridad externa de la República, además de las normas que regulan las facultades de otros poderes y órganos del Estado.
- **Artículos 39º y siguientes,** que regulan situaciones específicas que afectan el normal desenvolvimiento del Estado.

b. Leyes

- **Código Procesal Penal:** Regula el proceso de investigación y juicio criminal en Chile, y en ese marco, cualquier investigación relativa a ciberdelitos que sea llevada adelante en el país. Junto con ello, regula un conjunto de medidas intrusivas, que pueden afectar la vida privada o inviolabilidad de las comunicaciones de sus destinatarios, y por ende la confidencialidad de su información, para lo que la Ley exige requisitos legales a su respecto, junto con una orden judicial que autorice la práctica de dichas medidas.
- **Ley Nº19.913, crea la unidad de análisis financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos:** regula algunas medidas de investigación y vigilancia que, tal como en el caso Código Procesal Penal, pueden afectar la vida privada o inviolabilidad de las comunicaciones de sus destinatarios, y por ende la confidencialidad de su información, debido a lo también en este caso la Ley exige una autorización judicial aparejada al cumplimiento de los requisitos legales del caso.
- **D.L. Nº 211, Ley de Defensa de la Libre Competencia:** de manera idéntica al caso anterior, la Ley autoriza la práctica de diligencias intrusivas en casos específicos, que se regulan en los mismos términos ya expuestos.
- **Ley Nº19.974, sobre el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia:** en el marco de la recolección de antecedentes de inteligencia, esta Ley regula la práctica de procedimientos especiales de obtención de información, que deben efectuarse con

orden judicial previa y una serie de otros resguardos legales que limitan la obtención y uso de esta información.

- **Código Penal:** es el principal catálogo de delitos del país, contemplando la descripción de un conjunto de conductas específicas junto a las penalidades que se asocian a ellas. En el marco de la ciberseguridad, este Código contiene una serie de conductas que son susceptibles de cometerse a través del ciberespacio o afectar sus componentes, con lo que tiene una relevancia central en la formulación de políticas y combate al cibercrimen.
- **Código de Justicia Militar:** es un cuerpo legal que contiene disposiciones específicas relativas en su mayor parte a delitos cometidos por militares o en tiempos de guerra. Dentro de sus disposiciones, se contienen algunos delitos relativos al espionaje y revelación de información clasificada a terceros, que apuntan a la protección de la seguridad nacional.
- **Ley Nº19.223, tipifica figuras penales relativas a la informática:** dentro de los ciberdelitos, existe una subcategoría relativa a la afectación de los componentes lógicos del ciberespacio (programas de computación, sistemas informáticos, bases de datos), que se denominan delitos informáticos. Esta Ley contempla tipos penales específicos para el acceso no autorizado, sustracción y destrucción de sistemas de información.
- **Ley Nº 20.009 sobre Extravío, Robo o Hurto de Tarjetas de crédito y débito**
- **Ley Nº 18.168, ley general de telecomunicaciones:** esta Ley regula el marco jurídico del sector de las telecomunicaciones en el país, que proveen de infraestructuras físicas y lógicas claves para el desarrollo del ciberespacio nacional. Dentro de sus disposiciones, destaca la protección la confidencialidad e integridad de la información mediante la tipificación de delitos de interceptación no autorizada (art. Nº36B letras b y c). Cobran también especial relevancia para la ciberseguridad del país dos modificaciones recientes, correspondientes a la **Ley Nº20.453, que consagra el principio de neutralidad en la red para los consumidores y usuarios de internet,** que regula las medidas de gestión de red que puede adoptar un prestador de servicios de Internet, junto con establecer un deber de confidencialidad; y la **Ley Nº20.478, sobre recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones**, promulgada tras el terremoto que afectó a Chile año 2010, y que como su nombre señala, establece medidas que permiten mantener la continuidad de las telecomunicaciones en el país y, con ello, la disponibilidad de la información contenida en el ciberespacio.
- **Ley Nº19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma:** regula el uso de documentos electrónicos en el país y, con ello, mecanismos para asegurar la integridad y confidencialidad de la información, mediante el uso de mecanismos de firma digital, junto con un sistema que garantice el apropiado funcionamiento de quienes prestan estos servicios.
- **Ley Nº20.285, sobre acceso a la información pública:** crea un régimen de transparencia para las actividades del Estado, con obligaciones de transparencia activa, que debe efectuarse a través del sitio web de cada organismo público afectado; y pasiva, consistente en los datos que puede requerir cualquier persona a estos organismos, en la medida que no afecte otros derechos e intereses establecidos en la ley, como la seguridad del Estado o la privacidad de terceros, de manera tal que no se afecte la confidencialidad de la información en juego.

- **Ley Nº19.628, sobre protección de la vida privada:** establece un conjunto de principios y derechos relativos al manejo de datos personales en el país que puede exigir un titular de datos personales a quien posea o administre un registro de los mismos, junto con reglas de aplicación general para el manejo de datos personales por el sector público y privado, en torno al resguardo de la confidencialidad de esa información.

c. Decretos

- **D.S. Nº83/2005, aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos:** este decreto, desarrollando lo establecido en la Ley Nº19.799, establece una norma técnica aplicable a la administración pública, respecto de la seguridad y confidencialidad de los documentos electrónicos, y con ello, también de su infraestructura de la información, basada en el estándar ISO 27.000 y, junto con ello, estableciendo medidas administrativas como la creación de comités de la seguridad de la información en cada servicio público. Complementa a este decreto el **D.S. 93/2006, que aprueba norma técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la administración del estado y de sus funcionarios,** y que como su nombre describe, regula medidas orientadas a prevenir la recepción de SPAM en las casillas electrónicas de la administración del estado.
- **D.S. Nº1.299/2004, establece nuevas normas que regulan la Red de Conectividad del Estado que administra el Ministerio del Interior y fija los procedimientos, requisitos y estándares tecnológicos para la incorporación a dicha red de instituciones públicas:** este decreto, teniendo como antecedente la ley de presupuestos para el año 2005 y el D.S. 5996/1999, consolida una intranet denominada Red de Conectividad del Estado, en la que deberán inter conectarse una serie de ministerios y organismos públicos. Esta red centraliza el acceso a Internet y debe cumplir con estándares técnicos de seguridad acordes con los estándares del IEEE e ISO.
- **D.S. Nº1/2015, aprueba norma técnica sobre sistemas y sitios web de los órganos de la administración del Estado:** actualiza las normas técnicas para los sitios web de la administración del Estado, regulando condiciones de confidencialidad, disponibilidad y accesibilidad de la información contenida en dichos sitios, todas condiciones centrales para la ciberseguridad.
- **D.S. Nº533/2015, crea comité interministerial sobre ciberseguridad:** crea un Comité interministerial con el objetivo de preparar una propuesta de Política Nacional de ciberseguridad, del que forma parte el presente anexo.

a. Ministerio del Interior y Seguridad Pública

Entidad	Rol	Misión
Subsecretaría del Interior	Preventivo Formulador de Política Pública	El Ministerio del Interior y Seguridad Pública tiene la misión de resguardar la seguridad pública, y en tal sentido coordina, evalúa y controla la ejecución de planes intersectoriales en materia de prevención y control de la delincuencia (Art. 1 Ley N°20.502), entre ellas las que corresponden a los ciberdelitos, estableciendo políticas públicas para prevenirlos, enfrentarlos y sancionarlos. El Departamento de crimen organizado en particular, es responsable de elaborar estrategias para el combate del cibercrimen (Res. Exenta 10168, 3/12/2013)
Subsecretaría del Interior	Preventivo Reactivo Formulador de política pública	En virtud del Decreto Supremo N° 5996 de 1999, es el MISP el encargado de implementar y operar a nivel nacional, a través de la División de Informática, la Red de Conectividad del Estado (RCE). En complemento al decreto anterior, el Decreto Supremo N° 1299 del de 2004, faculta a esta cartera de Estado, para publicar o difundir las normas oficiales de la República en materia de seguridad de la información y establecer normas, estándares y políticas de seguridad lógica que en forma obligada deberán cumplir las instituciones públicas que se participan de la RCE, estando habilitada además para solicitar consultas de carácter técnico a cualquier institución del Estado. Cabe destacar la labor de la RCE como herramienta de apoyo a la ciberseguridad gubernamental
PDI, Brigada Investigadora del Ciber Crimen	Preventivo e Investigativo	Encargada de la investigación de los delitos de conformidad con instrucciones del Ministerio Público, como es el caso de los ciberdelitos.
Carabineros, Departamento OS 9	Preventivo e investigativo	Encargados del orden público y la seguridad pública interior, su alteración debe ser prevenida e investigada, como es el caso de los ciberdelitos.
Agencia Nacional de Inteligencia	Preventivo	De acuerdo a la Ley 19.974 que regula su funcionamiento, entre sus tareas se encuentra: "proponer normas y procedimientos de protección de los sistemas de información crítica del Estado" Art 8, letra c)

b. Ministerio de Defensa Nacional

Entidad	Rol	Misión
Subsecretaría de Defensa	Formulador de política	La Subsecretaría de Defensa es la entidad responsable de generar y mantener actualizada la planificación primaria y políticas correspondientes para enfrentar los desafíos que la ciberseguridad plantea para la Defensa Nacional, y de asegurar la correspondencia de la planificación secundaria con ésta.
Estado Mayor Conjunto y Fuerzas Armadas	Preventivo y reactivo	Las instituciones de las Fuerzas Armadas están a cargo de proteger su propia infraestructura de la información, además de colaborar en las tareas de ciberseguridad que correspondan en relación con la seguridad nacional y el sistema nacional de inteligencia. El Estado Mayor Conjunto es el organismo de trabajo y asesoría permanente del Ministro de Defensa Nacional en materias que tengan relación con la preparación y empleo conjunto de las Fuerzas Armadas, y está a cargo de elaborar y mantener actualizada la planificación secundaria de la Defensa, junto con otras tareas relevantes para la ciberseguridad del país. Las Fuerzas Armadas, por su parte, están a cargo, acorde a la planificación realizada, de los planes institucionales y operativos que correspondan.

c. Ministerio de Transportes y Telecomunicaciones

La Subsecretaría de Telecomunicaciones, que genera políticas públicas y fiscaliza su cumplimiento en materia de telecomunicaciones, está a cargo de la implementación de la Ley 20.478, "Sobre Recuperación y Continuidad en Condiciones Críticas y de Emergencia del Sistema Público de Telecomunicaciones", lo que realiza a través del decreto 60/2012 que fija el Reglamento para la interoperación y difusión de la mensajería de alerta, declaración y resguardo de la infraestructura crítica de telecomunicaciones e información sobre fallas significativas en los sistemas de telecomunicaciones. Asimismo, esta subsecretaría es la encargada de fiscalizar que se respete el principio de neutralidad de la red consagrado en la Ley 20.453.

d. Ministerio de Economía, Fomento y Turismo

Se encarga de formular políticas públicas en materia productiva. La misión del Ministerio de Economía es promover la modernización y competitividad de la estructura productiva del país, la iniciativa privada y la acción eficiente de los mercados, el desarrollo de la innovación y la consolidación de la inserción internacional de la economía del país, de allí que la consideración de la ciberseguridad como un foco de desarrollo nacional sea considerada en la Agenda de Productividad, Innovación y Crecimiento.

e. Ministerio de Justicia y Derechos Humanos

Por el rol que le corresponde en la modernización del sistema de justicia, la promoción de las normas y políticas públicas orientadas a facilitar el acceso y la protección de los derechos fundamentales de las personas y la seguridad ciudadana, el Ministerio de Justicia y Derechos Humanos debe en este contexto velar por la constante actualización y adecuación técnica de la legislación a los desafíos que impone el desarrollo tecnológico.

f. Ministerio de Relaciones Exteriores

Con el rol de articulador en la comunidad internacional y coordinador internacional de la política nacional de ciberseguridad, la Dirección de Seguridad Internacional y Humana del Ministerio (DISIN) identifica, coordina y promueve la posición e intereses de Chile en la comunidad internacional en materia de ciberseguridad, en todas sus dimensiones. Asimismo, coordina y promueve la participación de Chile en organismos y foros internacionales especializados (*Meridian, Octopus)*, OEA, UNASUR, UIT, IGF, Grupos de expertos ONU, entre otros). Fomenta además las relaciones bilaterales en esta materia.

g. Ministerio Secretaría General de la Presidencia

En relación con la formulación de políticas públicas en materia de gobierno y desarrollo digital, el Ministerio Secretaría General de la Presidencia, a través de la actual Unidad de Modernización del Estado tiene como objetivo acercar el Estado a las personas, y en este contexto desarrolla la modernización del Estado y el Gobierno digital.

h. Universidad de Chile

Entidad	Rol	Misión
NIC Chile	Órgano técnico, administrador	NIC Chile es la organización encargada de administrar el registro de nombres de dominio .CL, y de operar la tecnología que permite que estos nombres funcionen de manera eficiente y segura, para que personas, empresas e instituciones puedan identificarse en Internet
CLCert	Órgano académico, punto de contacto con CERT internacionales y con FIRST	CLCert tiene como principales objetivos: Entregar en forma oportuna y sistemática información sobre vulnerabilidades de seguridad y amenazas. Divulgar y poner a disposición de la comunidad información que permita prevenir y resolver estos incidentes de seguridad. Educar a la comunidad en general sobre temas de seguridad, promoviendo las políticas que permiten su implementación.

i. Instituto Nacional de Normalización

Cumpliendo el rol de órgano técnico, normalizador de estándares y acreditador, el Instituto nacional de Normalización (INN), es una fundación de derecho privado sin fines de lucro, creada por CORFO en el año 1973, como un organismo técnico en materias de la Infraestructura de la calidad, las cuales en el ámbito de la ciberseguridad se relacionan con la serie de normas ISO/IEC 27000.

j. Ministerio Público

Cumpliendo el rol de dirigir la persecución penal y ejercer la acción penal pública, el Ministerio Público es un organismo autónomo, cuya función es dirigir la investigación de los delitos, llevar a los imputados a los tribunales, si corresponde, y dar protección a víctimas y testigos.

k. Poder Judicial

Con la facultad exclusiva de conocer resolver y hacer cumplir lo juzgado en causas civiles y penales, el Poder Judicial está conformado por tribunales de diversa competencia: civil, penal, laboral y familia. En el marco de la ciberseguridad, los jueces autorizan algunas diligencias intrusivas, controlan la legalidad de la investigación penal, y deciden respecto de las causas criminales, incluyendo los ciberdelitos.

Anexo Nº2: Panorama de riesgos y amenazas

1. FUENTES Y TIPOS DE RIESGOS Y AMENAZAS

En atención a la naturaleza global del ciberespacio, los riesgos provienen de amenazas provenientes tanto de Chile como del exterior, y poseen diversos orígenes, entre los que destacan para nuestro país:

- **Incidentes internos:** fugas involuntarias de información, interrupción accidental de sistemas informáticos, u otros incidentes involuntarios que pueden afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información.
- **Desastres naturales o fuerza mayor:** terremotos, inundaciones u otros desastres que puedan afectar al ciberespacio, debido a la destrucción de infraestructuras físicas esenciales para la disponibilidad de la información.
- **Actividades de espionaje y vigilancia llevadas a cabo por actores estatales:** conductas que afectan la confidencialidad de la información, mediante su sustracción con fines políticos o estratégicos. En particular, destacan acciones utilizando herramientas sofisticadas conocidas como APT (amenazas avanzadas persistentes), que a su vez pueden valerse de vulnerabilidades informáticas no publicadas de las tecnologías en uso.
- **Ataques de denegación de servicio y denegación distribuida de servicios (DOS y DDOS):** consisten en la sobrecarga intencional de servicios que se proveen en un sistema informático, que puede ser conducida desde un punto de la red o distribuirse para coordinar el ataque desde varios puntos, muchas veces mediante dispositivos infectados con programas maliciosos, con el fin de cumplir dicho propósito.
- **Cibercrimen:** actividades criminales cometidas contra componentes del ciberespacio (acceso no autorizado, sabotaje de información, robo de información, secuestro de información o *ransomware* o empleando herramientas del ciberespacio como medio de comisión *phishing, pharming*, fraudes virtuales, y otros relacionados).
- **Ataques a infraestructuras críticas mediante el ciberespacio:** la alteración en el funcionamiento de infraestructuras críticas (físicas o de la información) realizada por medios electrónicos. Por ejemplo: disrupción masiva de sistemas financieros, intervención de servicios básicos, daños físicos a infraestructuras físicas, y otros relacionados.

Todos estos riesgos y amenazas afectan la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información en el ciberespacio, y en el mediano plazo, puede afectar el desarrollo del país en el ciberespacio, privándonos de los beneficios asociados al gobierno digital, comercio electrónico, formas de organización social facilitadas por el ciberespacio, y amenazando la seguridad de las personas e instituciones en este ambiente. Algunos casos pueden caer en más de una categoría de las aquí presentadas.

2. RIESGOS Y AMENAZAS EN EL CONTEXTO GLOBAL

A nivel global, existen abundantes antecedentes sobre ciberataques consistentes en actividades de espionaje y ataques de denegación distribuida de servicio (DDoS) en Internet, entre otros. Asimismo, la interceptación masiva de redes de telecomunicaciones, la inutilización del servicio de Internet, el espionaje contra gobiernos y empresas, además de ataques contra infraestructuras críticas como bancos y servicios gubernamentales han marcado la pauta informativa. También existen antecedentes de abusos de requerimientos legales de datos a diversos proveedores de productos servicios digitales por parte de los países donde están radicados los mismos.

Dentro de estos casos, destacan: Irán (2010), cuyas centrífugas nucleares fueron inutilizadas por un virus informático diseñado para tal efecto; Estonia (2007), donde parte de su infraestructura crítica fue inutilizada por semanas; las revelaciones de Edward Snowden (2013) sobre espionaje masivo por parte de las agencias de inteligencia de Estados Unidos, cuya extensión aún permanece incierta por la cantidad y periodicidad de estas revelaciones; y el espionaje contra empresas de defensa (Lockheed, 2011) y entretención (Sony, 2014) del mismo país, cuya extensión compromete gravemente intereses económicos y derechos fundamentales de las personas a lo largo del mundo.

3. RIESGOS Y AMENAZAS EN EL CONTEXTO REGIONAL

A nivel regional, países que han registrado el mayor número de ciberataques en Latinoamérica fueron Brasil, Argentina, Colombia, México y Chile. Los accesos o robo de información desde un ordenador infectado -denominados *botnets*- predominaron en la región. Incluso, un tipo específico de este código malicioso llamado *dorkbot* generó más de 80 mil acciones contra el sistema virtual, concentrándose en Chile (44%), Perú (15%) y Argentina (11%).[17]

4. ACTIVIDADES MALICIOSAS DETECTADAS EN LA RED DE CONECTIVIDAD DEL ESTADO

En Chile, la Red de Conectividad del Estado (RCE) sufre numerosas actividades maliciosas o sospechosas. Existe registro de incidentes vinculados a ataques de denegación distribuida de servicios (DDoS) o alteraciones de sitios webs gubernamentales, observándose un importante crecimiento de éstos desde el año 2010. Asimismo, en el año 2015, a nivel general, los administradores de la red gubernamental detectaron los siguientes patrones maliciosos:

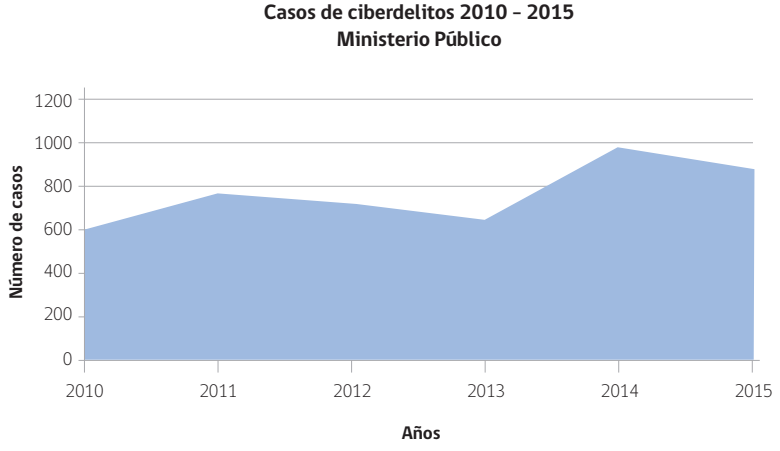
17 Prandini, P. y Maggiore, M. 2013. Op. Cit.

Cantidad de Registros	Descripción
58.375.435	Intentos de acceder a información de dispositivos de red mediante protocolo de administración SNMP
45.903.511	Escaneo de puertos de administración de dispositivos de la plataforma switch, router o seguridad.
19.745.086	Flujo web con traspaso de contraseñas en texto claro (sin cifrar)
7.805.544	Detección de actualizaciones dinámicas de DNS
5.570.661	Detección de flujo TFTP (transferencia de archivos) usando protocolo tftp
4.463.394	Detección de flujos portmap
3.359.194	Detección de trafico anómalo por el puerto de los DNS
2.479.277	Detección de flujos de escritorio remoto
2.077.435	Detección de consultas DNS por dominios reconocidos como de uso de malware
2.023.403	Detección de reconocimiento por PING
1.451.708	Escaneo de puertos de administración de dispositivos de la plataforma switch, router o seguridad.
1.428.461	Detección de acceso a wordpress (componentes claves)
1.400.697	Detección de malware MORTO
1.120.311	Detección de tráfico NO cifrado a través de puerto tradicionalmente utilizado para transmitir cifradamente (443)
1.106.303	Detección de acceso a zonas prohibidas de sitios web
1.025.252	Flujo de credenciales en texto claro de login wordpress (utilizando en sitios web de gobierno)

Patrones detectados en la Red de Conectividad del Estado (RCE) durante el período 2015
(Fuente: División Informática del Ministerio del Interior, año 2016)

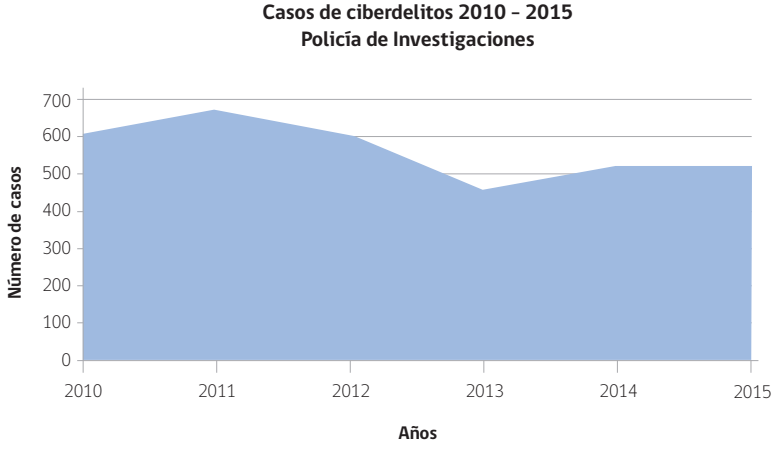
5. CIBERDELITOS EN CHILE

De acuerdo con el Ministerio Público, en relación con el cibercrimen, entre los años 2010 y 2015, el número de casos ingresados bajo el rótulo "delito informático" fue de 4.648 casos, distribuidos como se indica a continuación:



Casos ingresados por ciberdelitos 2010 - 2015 por Ministerio Público, referidos sólo a las figuras reguladas en la Ley N°19.223 (Fuente: ULDDECO, Ministerio Público, 2016[18]).

Por su parte, según los datos aportados por la Policía de Investigaciones (PDI), durante el periodo 2010 - 2015, se realizaron un total de 3.370 investigaciones, distribuidos como se indica a continuación:



Investigaciones efectuadas por ciberdelitos 2010 - 2015 por PDI (Fuente: Brigada de Cibercrimen, PDI, 2016).

18 Ministerio Público de Chile. Breve sinopsis acerca de la actual regulación y punibilidad en Chile de los denominados Ciberdelitos. Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado. Tal como indica el documento señalado, los datos presentados no constituyen el número total de ingresos por los casos, debido a que muchos de ellos ingresan rotulados como estafa (página 6).

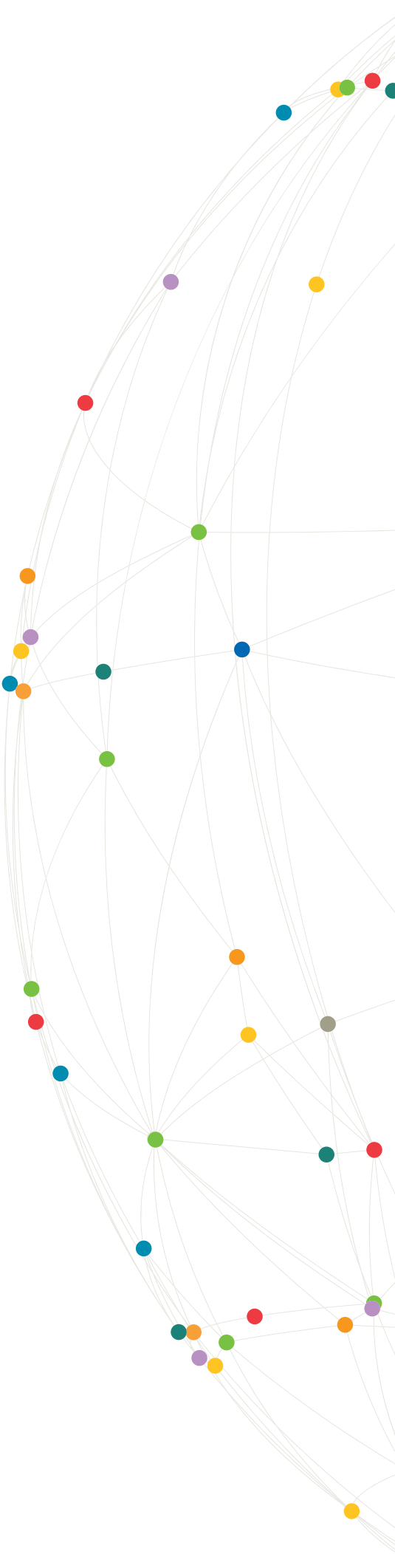
Por su parte, Carabineros identifica diferentes tipos de ilícitos en el ciberespacio a nivel nacional, siendo los más comunes el acceso indebido a sistemas; la adquisición, comercialización y almacenamiento de material pornográfico infantil; sabotaje informático; y transacciones bancarias ilícitas *(phishing)*.

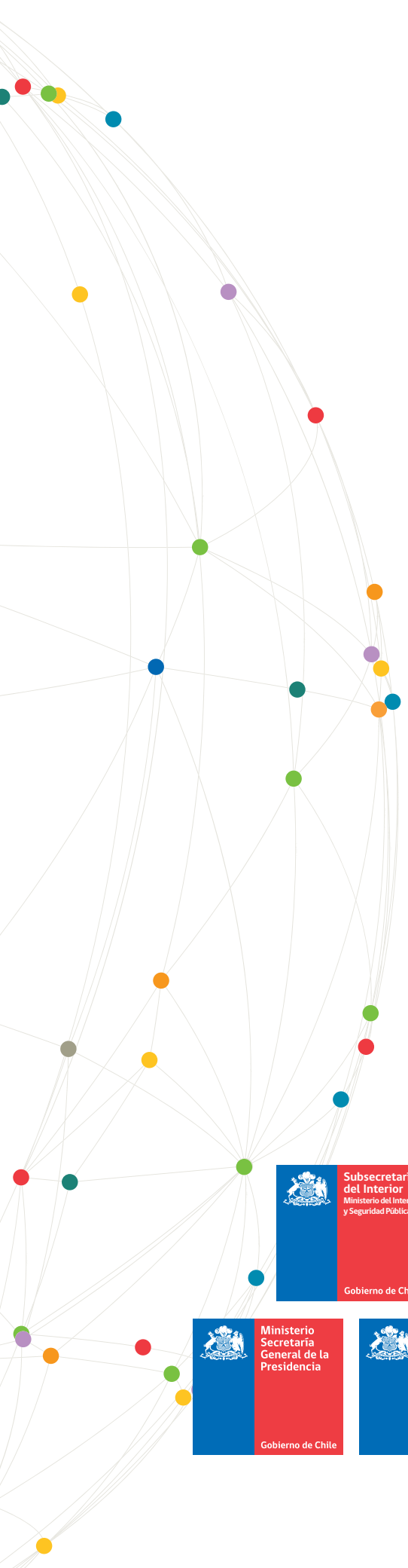
Asimismo, los cibercrímenes cometidos en Chile confirman el carácter transnacional de los ilícitos en el ciberespacio, específicamente, en el uso fraudulento de tarjetas de crédito y débito, con la detección de personas de diferentes nacionalidades, en la planificación y comisión de dichos delitos.

Conclusión

Los antecedentes expuestos constituyen una amenaza para la confidencialidad, integridad disponibilidad y trazabilidad de la información en el ciberespacio, y afecta a todos sus usuarios, impidiéndoles utilizarlo de manera segura, vulnerando secretos estatales y comerciales, y amenazando los derechos fundamentales de las personas, especialmente aquellos vinculados con la protección de su vida privada e inviolabilidad de sus comunicaciones.

Lo anterior hace imprescindible contar con políticas de gestión y minimización de riesgos que consideren estos riesgos y amenazas, especialmente en lo relativo a las infraestructuras críticas de la información, considerando reglas especiales para la adquisición y operación de soluciones tecnológicas que tomen en cuenta el contexto internacional existente en materia de ciberseguridad.





CICS Comité Interministerial sobre Ciberseguridad

www.ciberseguridad.gob.cl

Subsecretaría del Interior
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Ministerio de Relaciones Exteriores
Gobierno de Chile

Subsecretaría de Defensa
Gobierno de Chile

Ministerio de Hacienda
Gobierno de Chile

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

Ministerio de Economía, Fomento y Turismo
Gobierno de Chile

Ministerio de Justicia y Derechos Humanos
Gobierno de Chile

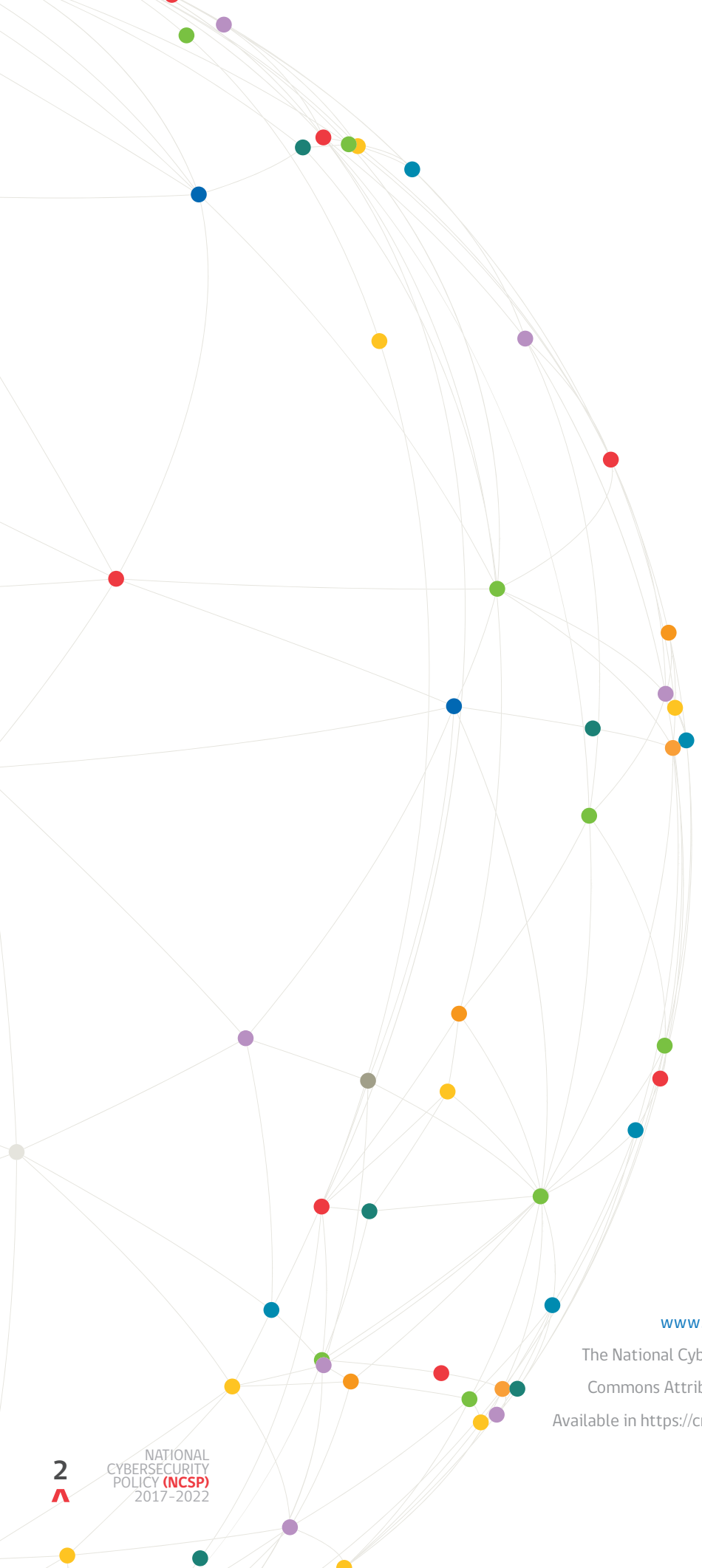
Subsecretaría de Telecomunicaciones
Gobierno de Chile

Agencia Nacional de Inteligencia
Gobierno de Chile

NATIONAL CYBERSECURITY POLICY

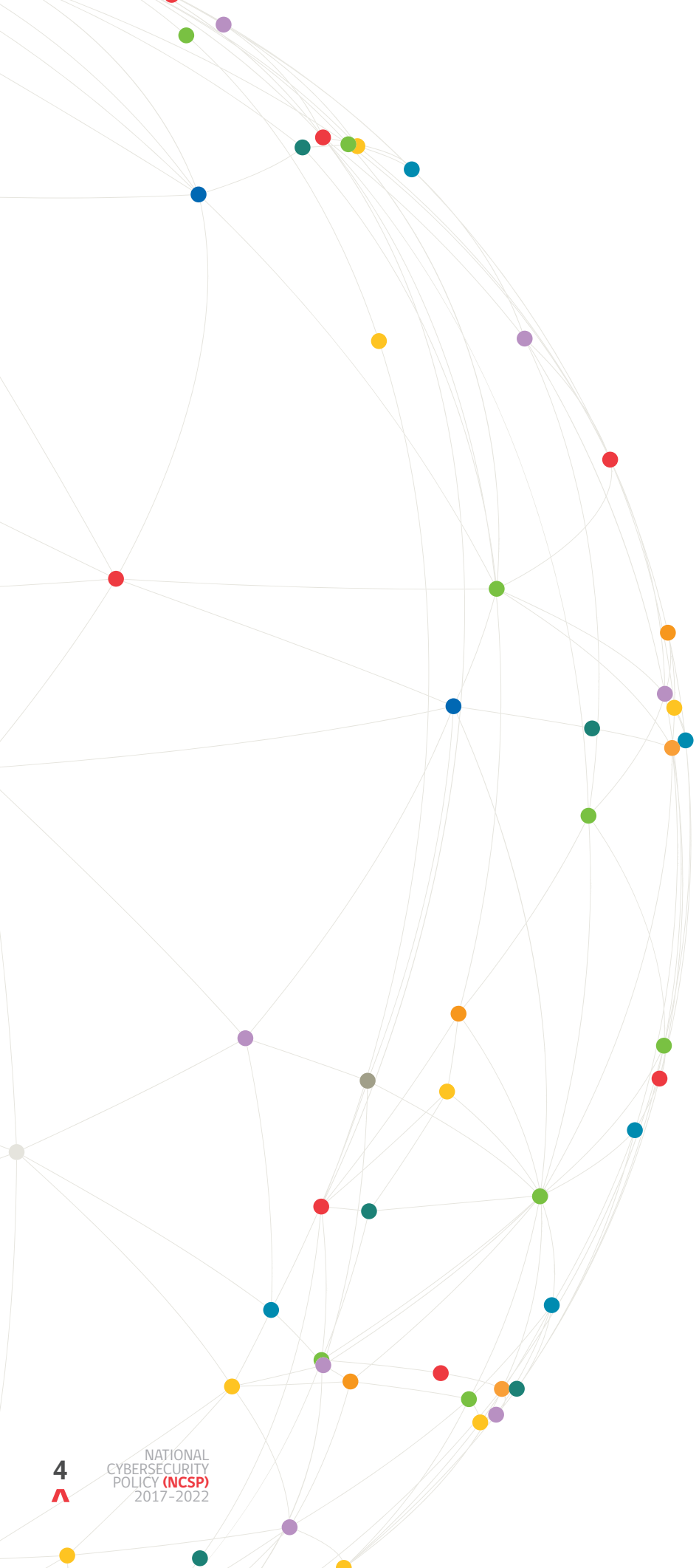
Gobierno de Chile

www.gob.cl



www.ciberseguridad.gob.cl

Table of contents



A Cyber-Security Policy for Chile

Information and communication technologies (ICTs) are a set of tools like no other in history, that has helped people, and has improved organizational interaction, economic operations and both private and public communications.

Their impact has been deep and broad in our society, and their reach extends day by day. People's access to the Internet has grown a 45.3% in the last two years, from a 52.2% by 2014 to 73.8% by March of 2016. Our national digital economy has grown around 11% in the same period, from 34 billion dollars in 2014 to 39 billion dollars in 2015.

This impact has transformed also the way our people use and understand technology.

The ICTs have had a social effect with no precedents in history, allowing our citizens to get informed, to organize themselves, and to participate from social life. Particularly, our children and adolescents make intensive use of social networks.

A transformation of this magnitude brings forth important challenges for our State, as it is imperative that all of this technology and its potential is used mainly to serve our people. We need to democratize the usage of the Internet, and to transform it into a tool for inclusion, efficiency and certainty, by ensuring the security and privacy of all those who use it everyday.

Chile must stay up-to-date in security matters, as any mistake, or any successful breach to our systems, may harm our people's welfare or our rights, it may negatively affect our interests, or it may hinder or even impede the operation of critical services for the country.

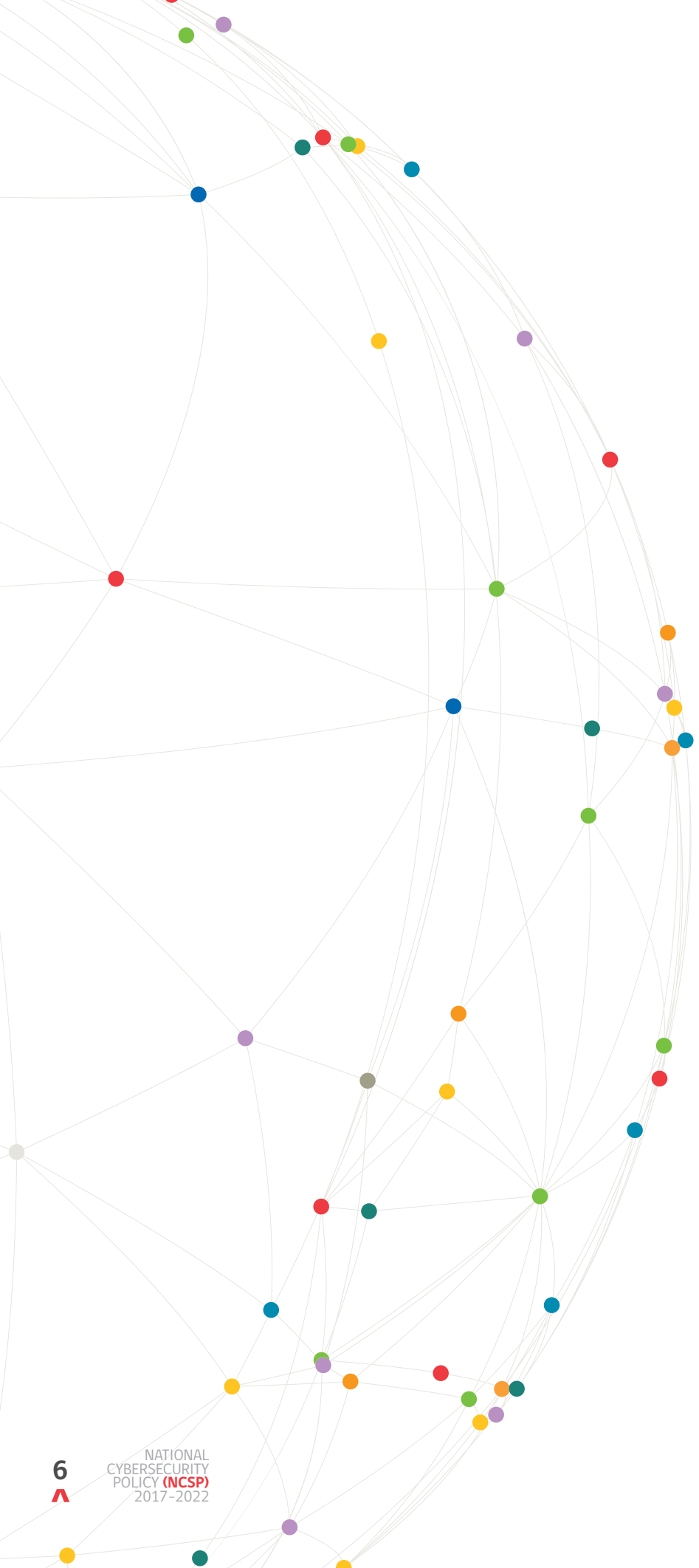
Listening to this demand, my government program included the development of a Digital Security Strategy, in order to protect both private and public interests in the digital realm.

This commitment was confirmed in November 2015, when we presented the Digital Agenda 2020, wherein it was announced the creation of a digital security strategy which, finally, is being released today through this document.

This first policy was designed from an intense dialog between private and public parties. For months we listened to public services representatives, professional and labor guilds, researchers and experts from within and abroad. When the Interministerial Committee wrote the first draft of this policy, it was subject to a public hearing as mandated by Law 20.500 about public participation. Numerous contributions were received which, no doubt about it, helped to improve it.

The national policy sets concrete goals and commitments for the overarching purpose of promoting and ensuring a free, open, safe and resilient cyberspace. A space that we expect it may allow our fellow citizens to reach their maximum potential. As it also happens with the
Digital Agenda, and the Productivity, Innovation and Growth Agenda, we expect this new policy to allow us to reduce the access gap, to increase awareness about safe use of ICTs, and to ensure the sustained technological leadership our country has in the region.

Michelle Bachelet Jeria
President of Chile



ICT penetration in every area in which we develop and interact has brought about a revolution that has left no one indifferent. Today we can hardly think of life without computer networks and that includes, of course, our social relations.

In the public sector, the State increasingly transmits information and interacts with citizens via the Internet, thus promoting the digital government and fulfilling its commitments of timely delivery of services and transparency. Along with the latter and in order to facilitate internet access to its citizens, the State has created programs that enable free internet access through the program WiFi ChileGob, a project that helps improve access in remote locations through Chile. In addition, the government is promoting the initiative "I choose my PC", which seeks to increase equality and to bridge the digital divide by favoring vulnerable seventh grade children. This program has benefited more than 350,000 students. Since it was launched seven years ago.

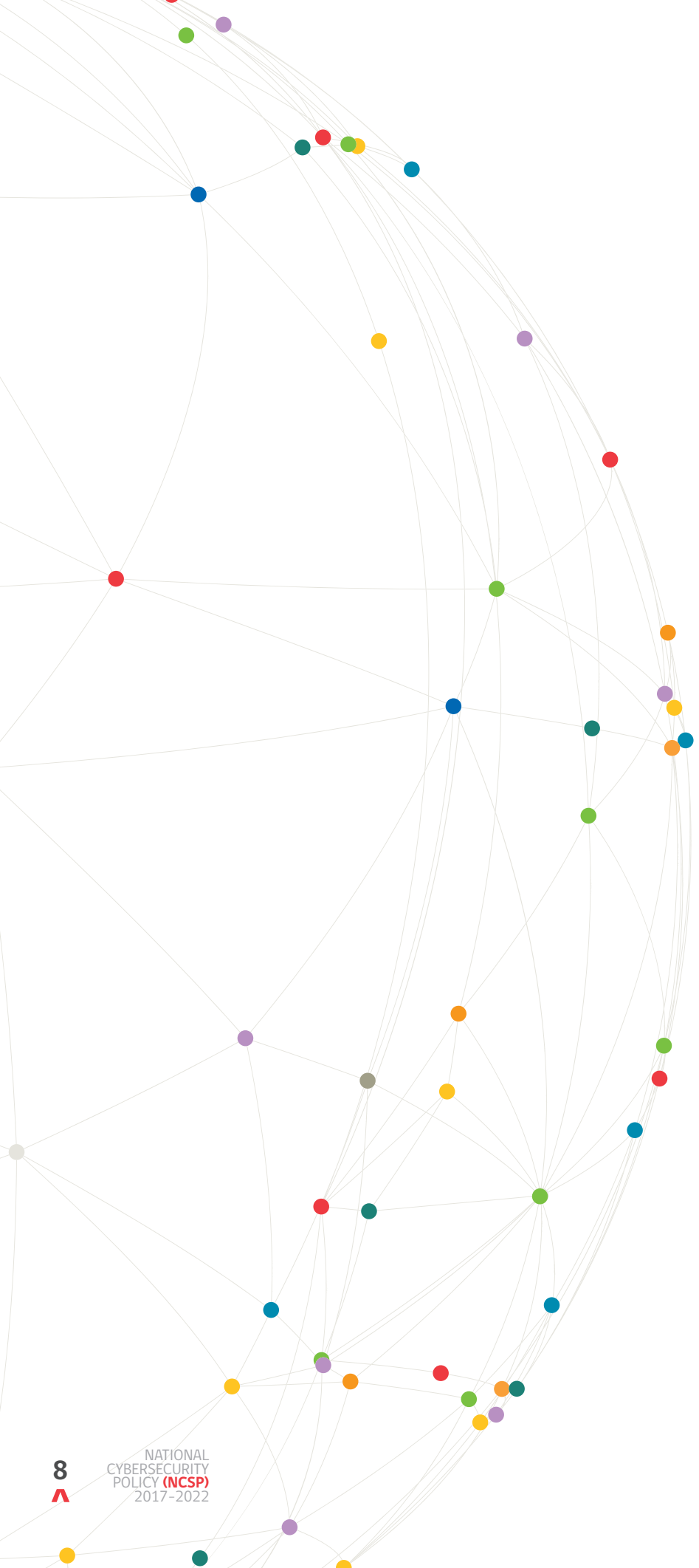
In this context, where Internet access and the use and dependence on ICT increases significantly, the criminological phenomenon associated with cyber crime and cyber attacks has worsened. For example, the State Information Network recorded an increase of more than one hundred million attacks, between 2014 and 2015, rising the 2016 to values exponentially higher by DDoS attacks.

In light of this reality, both the government of President Michelle Bachelet and the Digital Agenda 2020 in particular consider the development of a digital security strategy that promotes protection of private users. Therefore, the government has worked since April 2015 through an Inter-Ministerial Committee on Cybersecurity, on the development of Chile's first National Cybersecurity Policy, which has been fine tuned after a successful Citizen Consultation process carried out between February and March 2016.

While the National Cybersecurity Policy addresses with particular interest the prosecution and punishment of cybercrime, it goes far beyond the punitive area, for a fundamental variable to reduce the risks associated with cyberspace and take advantage of its potential is awareness, training in and dissemination of cybersecurity among society. Likewise, exploiting the competitive advantages of our country in terms of internet access, digital market maturity and quality professionals, the Policy seeks to promote industrial and productive development in cybersecurity.

Thus, I am convinced that the implementation of the measures contained in the cybersecurity policy as well as the State guidelines that it considers will contribute to further development of interagency cooperation and public-private partnership, which will enhance the value of free, open and safe cyberspace as a way to achieve greater economic development of our country and greater welfare for all Chilean people.

Mahmud Aleuy Peña y Lillo
Undersecretary of the Interior
Chairman of the Interministerial Committee on Cybersecurity



It has been a long time since cyberspace ceased to be part of science fiction to become one of the main areas of social interaction. Without going any further, Chile has the highest rate of Internet penetration in Latin America, with more than 70% of its population connected.

This has allowed its people to use digital technologies intensively to communicate with one other, express their ideas, share their causes or strengthen personal ties through social media, to carry out multiple transactions online and to take advantage of e-commerce facilities. However, this intensive use also increases our levels of dependence on the internet and the infrastructure that supports it, exposing us to new risks and threats.

Therefore, one of the challenges undertaken by the Government has been to improve the standards of digital security of our country, in order to protect people and the exercise of fundamental rights such as privacy, freedom of expression and access to information, among others.

This policy is the first concrete result of this challenge, a result that is the fruit of collective work that we assumed in the Interministerial Committee on Cybersecurity, made up by the Undersecretariats of Interior, Foreign Affairs, Defense, Finance, General Secretariat of the Presidency, Economy, Justice, Telecommunications and the National Intelligence Agency. The Committee met throughout 2015, holding multiple public hearings where it welcomed representatives from trade associations, companies, civil society, academics and national and international cybersecurity experts.

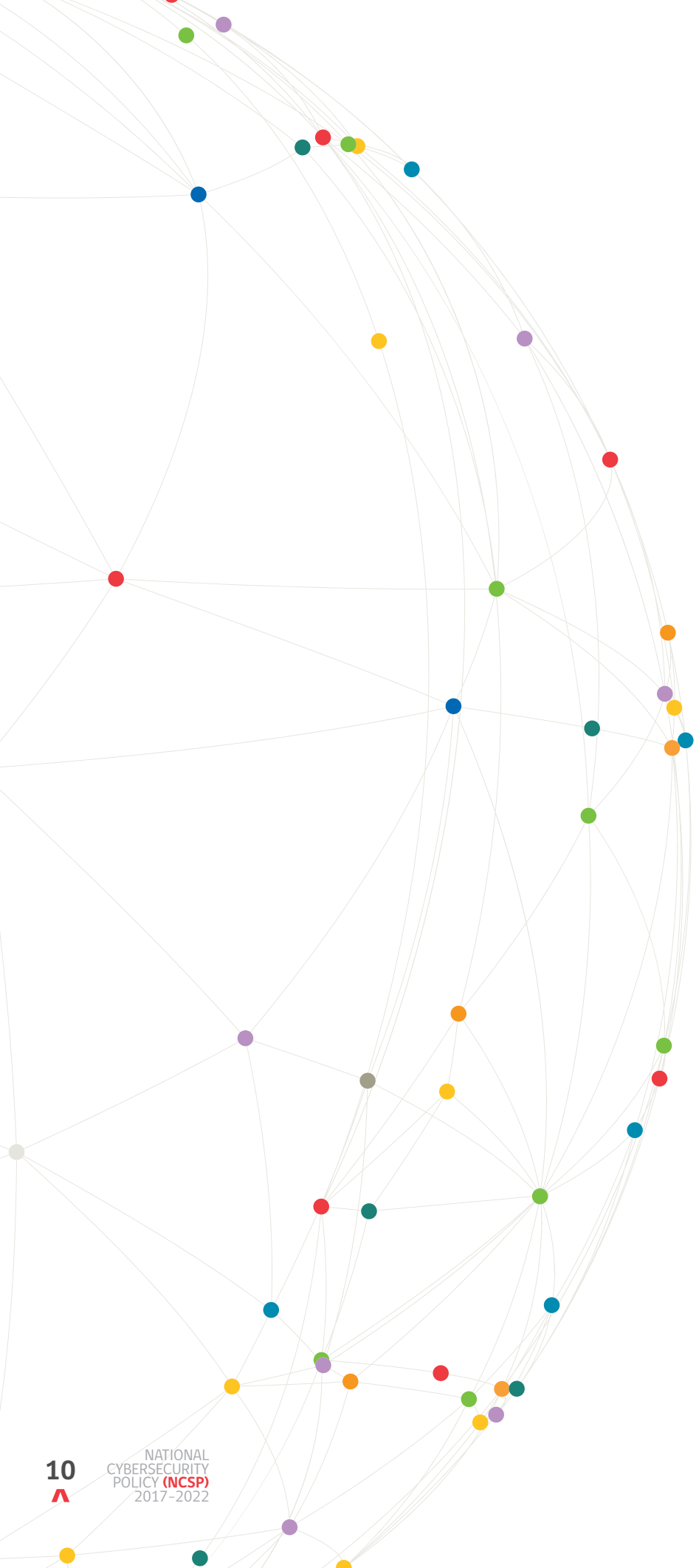
This policy was subject to an extensive public consultation process, through which fifty observations, comments and criticisms were received which certainly enriched the document that you have at hand.

The policy outlines five strategic long-term goals, aimed at addressing the challenges that our country faces in cyberspace, incorporating not only the scope of action of the State but also considering the role of the private sector, the civil society and the academia in this important task.

The policy reflects a central tenet: security and freedom are complementary. Combating cybercrime and other threats on the Internet cannot become an excuse to trample human rights such as privacy and freedom of expression on the contrary, they are means to fully guarantee these rights in cyberspace.

Now we face the great challenge of implementing the policy and monitoring its effectiveness, for which it is essential to have the cooperation of all stakeholders, so that our country can further progress in building an open, free and safe cyberspace for all.

Marcos Robledo Hoecker
Undersecretary of Defense
Executive Secretary Interministerial Committee on Cybersecurity



2 Introduction

The massive use of information and telecommunication technologies (ICT), while contributing to the country's development, also entails risks that may affect people's rights, public security, critical infrastructure, digital government, and Chile's essential interests and foreign policy.

These risks may arise from multiple sources and be translated into a series of activities including espionage, sabotage, fraud or cyber attacks carried out by, *inter alia*, other countries, organised groups or individuals.

There is important progress at an international level in the management of ICT-related risks. By 2015, over 40 countries had developed a cybersecurity[1] strategy or policy -some of which are already working on their second or third version. Note has also been taken of the important evolution in terms of doctrine, techniques and regulations within the most diverse organisations and international forums.

At a national level, the challenge lies on developing a policy driving the country's actions in cybersecurity matters, together with implementing and adopting the measures required to protect user security in the cyberspace, by taking into account educational strategies focused on self-care and prevention in the digital environment, and complying with President Michelle Bachelet's programme of government -which proposes **"to develop a digital security strategy protecting private and public users"**[2].

This document contains the political guidelines developed by the Chilean State in the field of cybersecurity, with a view to 20223, and aimed at having a **free, open, safe and resilient cyberspace.**

1 Further information in the following websites:
https://ccdcoe.org/strategies-policies.html
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/
http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx

2 President Michelle Bachelet's Government Programme, Page 57.

3 As explained in section V, "Roadmap", this policy contains long-term guidelines aimed at this and the coming government, and a series of short-term measures to be planned and executed by each relevant administration.

3 Why there is need for a national cybersecurity policy?

A. To protect people's security in the cyberspace

People are to be ensured a security level allowing them to carry out their normal personal, social and community activities in the cyberspace, such as well as to exercise their fundamental rights as freedom of speech, access to information, protection of the private life and personal property.

B. To protect the country's security

There is need to promote the safety of information networks and systems belonging to the public and private sector, especially the ones that are essential for the proper running of the country, ensuring there is continuity of basic services.

C. To promote cooperation and coordination between institutions

There is need to improve communication, coordination and cooperation actions between institutions, organisations and companies, both in the public and private sectors, at a national and international level, with the purpose of strengthening trust and provide a single answer to cyberspace risks.

D. To manage risks in the cyberspace

There is need to take into account the development of analysis and management processes for the use, processing, storage and transmission of information, as well as the building of capacities to prevent and recover from cybersecurity incidents that may arise, in order to achieve a stable and resilient cyberspace.

4 Current status of cybersecurity: regulations, institutions, risk overview

A. Regulations and institutions

The current institutional structure in the field of cybersecurity is based on different bodies and entities. This requires the strategic coordination of different efforts, and their roles and duties, as well as the establishment of common practices and technical criteria, with the purpose of improving efficiency and effectiveness in the field of cybersecurity[4].

The country has in place a set of legal and statutory regulations that relate directly or indirectly with the challenges of cybersecurity -which should be reviewed and updated in accordance with the guidelines set out in this policy and with Chile's international commitments, for example, Law No. 19,223 about cybercrime or Law No. 19,628 about the protection of private life, among other rights.

B. Risk overview

Because of the global reach of cyberspace, risks and threats may come from Chile and abroad, due both to natural and criminal activities, such as, for example, espionage and to surveillance actions carried out with different purposes, thus affecting the confidentiality, integrity and availability of information assets in the cyberspace and, therefore, people's rights[5].

At a global level, there is plenty of evidence about cyber attacks and online espionage. The large-scale interference with telecommunication networks, the outage of Internet services and espionage carried out against governments and companies, as well as attacks against critical infrastructure such as basic services, financial institutions and government entities have been openly covered in the global news.

Regionally, the countries affected with the highest number of cyber attacks in 2013 in Latin America were Brazil, Argentina, Colombia, Mexico and Chile. Accessing or stealing information from infected computers or devices were a feature in the region[6].

Likewise, cybercrimes perpetrated in Chile are a confirmation of their cross-border nature, especially such crimes associated with the fraudulent use of credit and debit cards and cyber frauds among others.

The policy takes into consideration this type of threats, especially the ones affecting the country's critical infrastructure.

---

4 See Annex No.1 with a detail of the regulations and institutional structure currently existing in the field of cybersecurity.

5 See Annex No.2 containing information about the risks of cyberspace.

6 Prandini, P. & Maggiore, M. 2013. Ciberdelito en América Latina y El Caribe. Una visión desde la sociedad civil (Cybercrime in Latin America and the Caribbeann. A view from the civil society). Proyecto Amparo, Sección de Estudios. LACNIC Registro de Direcciones de Internet para América Latina y Caribe. pp. 3.

5 Policy roadmap

This cybersecurity policy is composed of two core elements: a State policy containing objectives by 2022, and an agenda with specific measures to be implemented between 2017 and 2018.

The objective of this structure is proposing a general overview as to the direction the country should take in the medium and long term, with the development of a set of measures that may be implemented and evaluated during this Government's administration, thus leaving to the following administration the task of reviewing the policy and proposing an agenda that may be executed by the next administration.

A. Policy objectives for 2022

This policy sets out high level long-term objectives that allow driving the country's efforts to pursue such goals, serving at the same time as a guide to prioritise and rationalise the measures contained in this document.

Additionally, the policy includes a series of minimum essential roles and the corresponding institutional design that shall govern the same both in the short term and in the medium and long term (2017-2022).

B. Timetable of measures 2017-2022 and evaluation

Upon development of the policy objectives, a timetable is proposed for implementation in the 2017-2018 two-year period that will enable a joint effort from the Government and the private sector in the field of cybersecurity -focused on the adoption of prioritised measures and the preparation of a series of feedback that review and extend the policy's scope by the end of 2017.

C. Integrated supplementary policies in the digital field

This cybersecurity policy is an integral part of a set of policies implemented by the Government or at a development stage in the digital field with the purpose of having clear and systematic definitions about cyberspace.

> The Digital Agenda for 2020

The Digital Agenda for 2020[7] is a roadmap designed to guide the country's digital development through the definition of medium term objectives, lines of action and concrete measures. Launched in the second semester of 2015, this Agenda proposes that the widespread use of technologies becomes a means to reduce existing inequalities, with the opening of more and better opportunities for development and contributes to the respect of the rights of all Chilean women and men.

The Agenda includes a specific measure (No. 25) focusing on the development of a cybersecurity strategy which will be executed through this policy. Likewise, this policy is enhanced and supplemented by a series of measures contained in the Agenda, such as the support introduced in the new Law

7 Available in: http://www.agendadigital.gob.cl/

for the Protection of Personal Data, the safeguarding of Internet consumers, the development of a National Telecommunications Infrastructure Plan, and the upgrading of regulations governing the electronic signature, among measures.

> National cyber defence policy

Because the National Defence's networks and information systems are a critical infrastructure for external security and the exercise of the country's sovereignty, and by virtue of the constitutional and legal rights vested on the National Defence, during 2017 the Ministry of Defence will prepare and publish a set of cyber defence specific policies containing specific political definitions about how these networks will be protected and how the National Defence's capabilities may cooperate in the development of a free, open, safe and resilient space for the country.

> International cyberspace policy

One of the high level objectives of this policy relates with the international relations and cooperation about cybersecurity in the global context. However, it is essential for the country to incorporate these and other objectives, such as the development of human rights, defence, and other related objectives in order to consolidate and integrate the same into Chile's foreign policy.

With that in mind, this policy includes a specific measure related with the creation of a strategy in this field by the Ministry of Foreign Affairs which, in turn, is consistent with and executes measure No.11 of the Digital Agenda 2020 aimed at generating a country's widespread view about Internet governance.

6 Policy objectives by 2022

A. The country will have in place a robust and resilient information infrastructure, prepared to face and recover from cybersecurity incidents, under a risk management approach

> 1. Concept. Risk identification and management

Cybersecurity is described as a condition presenting the least risk for cyberspace -understood as a set of physical and logical infrastructure, and the human interactions taking place in the same. Within this set, the main feature to be protected is information confidentiality, integrity and availability which, in turn, create a robust and resilient cyberspace.

This framework does not include the increased capability of state or private surveillance actions by using digital technologies, which relate with public order or national security objectives and are discussed in other instruments having a different focus. Surveillance actions proposed in this instrument will only be aimed at managing the risks of information in the cyberspace.

Prevention and management models for cyberspace will be created from the Policy, including physical risks that may affect the same, regularly updated by a continuous improvement model, which shall be the basis for technical measures to be adopted in order to prevent, manage and overcome actual risks, with an emphasis on service resilience and continuity within a set deadline and focus on maximising the country's cybersecurity levels.

> 2. Protection of the information infrastructure

Information infrastructure is composed of people, processes, procedures, tools, installations and technologies supporting the creation, use, transport, storage and destruction of information.

There is an especially relevant group, within information structure, for a country to keep moving forward, called critical information infrastructure (CII), which includes the installation, networks, services and physical and information technology equipment whose impairment, degradation, rejection, interruption or destruction may have an important impact on the security, health and wellbeing of people and on the effective operation of the State and the private sector.

Special emphasis will be placed on the impact that an information security incident may have on physical infrastructures controlled or monitored from the cyberspace, and on the security of industrial surveillance sensors and devices enabling such actions.

CIIs shall the designed with an architecture maximising their robustness and resilience against events that may render them non-operational, and enabling them to adapt to natural phenomena, human interventions and information interferences such as non-voluntary incidents or cyber attacks.

> 3. Identification and prioritisation of critical information infrastructure

Sectors included in the definition of CII are very similar and recurrent in various international classifications. In Chile, while consideration of a specific policy for critical infrastructure is under consideration, information infrastructure in the following sectors will be considered as critical:

energy, telecommunications, water, health, financial services, public security, transport, the civil service, civil protection and defence.

The policy contains a full set of areas, roles and responsible State entities used to identify and specify the critical level of each sector.

Technical bodies in charge of executing measures derived from this policy shall include special cybersecurity standards for CIIs depending on the different levels of development, especially with regard to special processes.

The medium term will see the implementation of measures ensuring service continuity through the redundancy of the physical infrastructure of some CII, especially in the fields of telecommunications, civil service, civil protection and defence.

> 4. Equipment available to respond to cybersecurity incidents

According to best practices worldwide, it is essential to have available prevention, monitoring, management and response structures to face computer-related security incidents at a national level.

The basic body in this structure is the Computer Security Incident Response Team (CSIRT) or teams in charge of responding to computer security incidents. Chile needs today the human and financial resources, a clear institutional framework and a mechanism to operate in coordination so as to promote the creation and operation of the same at different levels of the national life.

Chile will have a national CSIRT in place to collect and structure information received from other (national and international) CSIRTs, promoting action coordination between CSIRTs in each sector, with the required authority to coordinate the technical response in the case of incidents endangering the country's security.

The Government's current CSIRT will be strengthened, with a specific CSIRT to be created in the area of the National Defence. Likewise, the need is also in place to evaluate the relevance of creating a CSIRT for critical infrastructure.

The creation of CSIRTs by sector will be supported by different public, private, academic and civil society stakeholders.

> 5. Implementation of standardised mechanisms for reporting, managing and recovering from incidents

There will be centralised and standardised mechanisms for reporting cybersecurity incidents enabling the widespread and real time overview of incidents generated in the country.

These mechanisms will be compulsory for the central Government and certain regulated sectors, and voluntary, in principle, for any stakeholders that may want to join them. The amount of information required will be restrictedly limited to what is needed to describe and manage the type of threat, especially avoiding the collection and processing of data affecting people's private lives.

For such purpose, the National CSIRT will keep a secure and confidential platform able to cooperate in case of cybersecurity incidents and gather the relevant information, and will create a network in conjunction with public and private bodies.

At the same time, both public bodies and CII will have institutional bodies responsible for information security, together management and recovery plans in place for addressing incidents, with special emphasis on business continuity and on minimising any damages caused by actual incidents.

In addition to the foregoing, the preparation of computer vulnerability reports by users and experts will be promoted through the adoption of guidelines for responsible information delivery, models to reward the detection of security problems, and other mechanisms promoting responsible disclosure.

> 6. Differentiated standards are required in the field of cybersecurity

Any information infrastructure governed by or providing goods and services to the Chilean Government, or services to the people, shall comply with a basic set of standards covering confidentiality, integrity and availability of the information and the systems operating the same, according to the risks and threats faced by them and in consistency with their size, maturity, critical state and confidentiality level of information and/or processes supported by them.

With regard to critical information infrastructure, any risk shall be properly evaluated and addressed pursuant to standards including CII's confidentiality, integrity and availability, aimed at having an effective and comprehensive security system in place that allows the prevention, management and recovery from cyber attacks and other information security incidents, together with contingency plans for ensuring business continuity of their services.

Standards and best practices used shall be compatible with international efforts ensuring the confidentiality, integrity and availability of information, without setting out specific solutions – except for qualified cases.

B. The State will protect people's rights in cyberspace

> 1. Crime prevention and trust building in cyberspace

Crime prevention, dissuasion, control and punishment are critical to minimise risks and threats in cyberspace, thus contributing to trust building in connection with the activities carried out within the same.

There are multiple criminal activities carried out in cyberspace such as stealing strategic information, interrupting online service systems, information hijacking (ransomware), phishing, pharming and the fraudulent use of credit or debit cards, among other illicit activities.

At a global level, there is information about cyber attacks consisting in espionage activities and distributed denial of service (DDoS) attacks through the Internet, the large-scale intercepting of telecommunication networks against critical infrastructure such as, *inter alia*, banks, basic services and Government entities. This policy is aimed at minimising risks associated to these threats.

In addition to public policies developed to prevent and punish the above-mentioned crimes, it is also possible to build trust in cyberspace by employing the same technologies. The adoption of technical solutions allowing to increase user security in cyberspace, especially in the case of solutions cooperating with identity management in this environment, such as the mass adoption of digital certificates (digital signature) in websites, and by people and organisations will be promoted as a way to safeguard user communication and identity.

This policy also recognises the value placed on encryption technology, thus allowing the provision of the most unprecedented levels of information confidentiality and integrity levels in history.

Measures based on this policy shall promote encryption adoption for online users according to international standards, and under no circumstances the intentional use of unsafe technologies shall be promoted, or there will be and obligation by any person or organisation to provide digital services to implement 'back door' mechanisms compromising or increasing any risks associated with the security technologies used.

> 2. Priority setting in the implementation of punishing measures

Unlike crimes committed in the physical space, cyberspace presents some challenges to crime prosecution and punishment. Some of these challenges include, *inter alia*, the identification of authors, the time elapsed between the perpetration of a crime and the victim's reaction, the low rate of complaints submitted and the unlike possibility to prosecute the perpetrator(s) -because enforcement agencies operate within the State's territorial borders while the cyberspace is essentially a borderless place.

Measures in place to punish these actions should be implemented by bearing in mind this context, and as a complement to this policy.

The updating of Chile's legislation, promoted by the decision to adhere to the Convention on Cybercrime of the Council of Europe[8], together with the upgrading and strengthening of current regulations and the development of cross-cutting measures instead of the adoption of measures by sectors, are important objectives in this field.

> 3. Multi-sectoral prevention

Because cyber attacks and cybercrime may be perpetrated by State bodies, organised groups or individuals, and threats may come from inside and outside the country, any response must come from multi-sectoral actors involving the private sector, the academia, the civil society and, indeed, criminal prosecution and defence bodies, as well as victim advocacy organisations.

It is therefore essential to generate the proper spaces for coordination, meeting and cooperation, and strengthen significantly the existing technical skills and access to training by prosecutors and judges, the investigation and forensic capacities of the police bodies, and the development of guidelines aimed at providing a minimum safeguard to the entire population.

Definitions must be designed to gather, standardise and integrate data and information related with cybercrime, increase investigation capacity and generate evidence regarding such crimes.

> 4. Respect for and promotion of fundamental rights

All measures proposed by the policy should be designed and executed with a focus on fundamental rights -because of their fundamental nature and indivisibility, and on the basis that cyberspace is an environment where people have the same rights as in the physical world[9]. Therefore, the policy includes and promotes the following:

8 Available in: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

9 In this regard, Resolution A/HRC/20/L.13 from the UN Human Rights Council declared that "people's rights should be also protected in the Internet".

- The Internet is a global public asset; therefore, users may not be deprived from accessing the network but for reasons of *force majeure* duly based, with access never being denied by vague reasons such as public order, national security, or for the honour of any individual despite their capacity or title.
- Regarding the foregoing, and taking into account that information availability is an essential characteristic of cybersecurity, this policy will support public and private efforts made for the access to information and culture by the population through digital channels.
- Related with the above, the principle of respecting Internet neutrality is also included, so that Internet service providers may not discriminate or arbitrarily restrict the access to any content whatsoever, unless there is a legal justification to do that.
- This policy also respects and promotes the respect for freedom of speech, by taking into consideration not only communication media but also the population as a whole, the intermediaries making possible to communicate these messages and social networks[10]. Any interference with this right shall be carried out in accordance with national and international standards in the field of human rights.
- The protection of private life and the inviolability of user communication in the cyberspace, including the protection against the unauthorised gathering, process and publication of personal data; transparency in the management of such data by private and public stakeholders, and as mentioned above, the protection of essential technologies to ensure that users may safely and confidently use the cyberspace.
- The protection of due process with regard to the measures affecting information security, seeking that surveillance and criminal prosecution measures in cyberspace comply with international standards with regard to protection such as the principles of suitability, need and proportionality[11]. These measures will not only be applicable to criminal prosecution by the State, but also to the actions of all its bodies, thus safeguarding the application of this right among the users of cyberspace. Massive and indiscriminate surveillance of cyberspace is a serious attempt against fundamental rights.

Efforts in the field of fundamental rights will especially take into account the rights of vulnerable groups, such as, *inter alia*, boys, girls and young people, the elderly, disabled persons and ethnic minorities. There will be also a gender focus making possible to visualise and address the inequalities faced by different users in cyberspace.

The policy will seek that all people may enjoy a safe cyberspace free from abuses such as online bullying, the theft of personal information, large-scale surveillance and other practices affecting especially the most underprivileged members of society. Particularly, efforts will be carried out at all levels so that cybersecurity is not considered luxurious for people or the country's organisations.

10 The role of Internet intermediaries has increasingly attracted attention because of the critical role they plan in ensuring rights such as freedom of speech. In this regard, reference frameworks such as the Manila principles may be consulted, [online] Available in https://www.manilaprinciples.org/es

11 A useful analysis tool is the document "*Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*" (International Principles about the Application of Human Rights to the Surveillance of Communications). [online] Available in: https://es.necessaryandproportionate.org/text

C. Chile will develop a cybersecurity culture based on education, good practices and accountability in the management of digital technologies

> 1. Cybersecurity culture

ICTs promote the development of an equitable and inclusive cultural, technological and economic heritage of the country and comprehensive people's development.

Therefore, a cybersecurity culture will be promoted at all levels with the purpose of making the tools and knowledge available for society to understand this field of human relations including its advantages and risks, and may manage them properly.

> 2. Community awareness and information

People will be made aware of the risks and threats involved in cyberspace with the purpose of achieving a safe use of platforms providing services to the community, both from public institutions and private agents.

The community will be made aware of the good use, measures or personal care and security in cyberspace.

> 3. Cybersecurity education

This field will present many challenges to Chile's educational system. Early and advanced education of the Chilean population should be a part of these challenges; therefore, digital gaps generated by, *inter alia*, inequitable access to resources, skills, infrastructure and connectivity should be addressed.

To achieve the above goal, it is critical to implement initiatives promoting and developing a **conscious, competent, informed** and **responsible** digital culture including all relevant stakeholders and understanding that this is a joint effort to achieve a common, long-term benefit.

D. The country will carry out cooperation actions with other stakeholders in the field of cybersecurity and will actively participate in international forums and discussions

> 1. Chilean foreign policy principles

Chile's foreign policy is based on a series of principles driving its diplomatic work and actions, such as: the respect for international law; the promotion of democracy; the respect for human rights; conflict prevention; the pacific resolution of disputes and the commitment to cooperate in the international arena. In turn, these principles drive the interest of Chile's foreign policy, namely: contribute to the strengthening of multilateralism and promote international peace and security[12].

The emergence of cyberspace, especially the Internet, as a public asset urges us to face the challenges of managing all types of risks, where interacting at an international level is particularly important in the light of the global and cross-border nature of the same.

Cybersecurity is a cross-cutting and multi-factorial concept which, at an international level, conveys the possibility to build common capacities, approaches and measures with the cooperation and

12 Further information in: http://www.minrel.gov.cl/minrel/site/artic/20080802/pags/20080802194424.html

assistance of other countries, such as the conviction that sustained multilateral diplomatic work involving multiple stakeholders allows decreasing the risk of conflict in cyberspace.

To achieve the above, the Ministry of Foreign Affairs will be responsible for coordinating with other ministries and Government agencies the international cybersecurity policy.

> 2. Cooperation and assistance

Bilateral cooperation work will promote different types of relations with other countries in the field of cybersecurity, including assistance to and from Chile, exchange of information and experiences, the implementation and furtherance of mechanisms for facilitating political dialogue in this field, and the promotion of transparency and trust building in cyberspace, with an emphasis on multi-agency work.

> 3. Reinforce the participation in multilateral and multi-stakeholder work

Efforts must be focused on promoting digital as a free, open and safe environment for all users in the cyberspace.

The country needs to strengthen its work in this field, taking into consideration the special challenges faced in terms not only of the technical conditions, and the global nature and decentralised character of the network, but also regarding its political scope, and with a system of Internet governance including multiple stakeholders where the private sector and civil society have a special role.

Within this framework, the country's involvement will be increased in the multilateral and global arena, supporting regional, sub-regional and multilateral consultations in this field, especially in Latin America, and actively involving stakeholders in this debate.

> 4. Promote international regulations encouraging trust and security in the cyberspace

Although there are practically no specific regulation instruments, the cyberspace is actually regulated both by the existing national laws and by the general applicable international regulations; therefore, the challenge lies particularly on being able to identify and interpret the relevant regulations of the applicable international law.

However, there are some challenges that must be faced through specific international agreements and regulations, such as the Convention on Cybercrime, which the country will adhere to, with reservations and safeguards consistent with this policy.

Additionally, the debate and adoption of multilateral and bilateral agreements should be promoted in order to encourage cooperation and mutual assistance in the field of cybersecurity, both in terms of formal instruments and as informal agreements and arrangements focused on international transparency and the trust building in this field.

E. The country will promote the development of a cybersecurity industry serving its strategic objectives

> 1. The importance of innovation and development in cybersecurity

Activities aimed at protecting domestic security and foreign defence generally require a strong innovation and development element promoting an increased development of the industry at a

national level. Within this framework, the field of cybersecurity requires a special effort because of its original nature and strategic importance for the country as a whole.

> 2. Cybersecurity as a means to contribute to Chile's digital development

While the size of the ICT sector represents 3~4, 12% share of the Chilean economy, in OECD countries this industry reports an average 6% share in the country's economies[13], generating a gap between both realities that Chile will partly resolve through the development of the cybersecurity component within this industry.

This will generate both an increased demand on the information technology industry and a higher industrial development in this field, helping the country to advance towards OECD's indicators, as well as strengthening policy objectives.

> 3. Development of the cybersecurity industry in Chile

There are no specific figures regarding the level of development of the national industry apart from some studies exploring this alternative[14]. The country's effort to develop a cybersecurity industry will be supported by studies describing the industry and identifying strategic fields for development in the short, medium and long time.

Particularly, a field which is regularly developed in compared experiences is the domestic industry related with the development and use of encryption standards by reason of its strategic importance for the country's security abroad.

> 4. Contribute to the generation of an offer by the local industry

Measures will be adopted in order to help creating and strengthening a domestic industry for cybersecurity services, technologies and management through a programme and initiatives aimed at the production of new goods and services in this area. A development pole will be created in this area which is in line with the Productivity, Innovation and Growth Agenda[15] and the Digital Agenda for 2020.

> 5. Generation of demand by the public sector based on the State's strategic interests

The generation of demand by the public sector based on their strategic and security needs and interests will support the strengthening of a national industry focused on cybersecurity services, technologies and management which is in line with international technical standards.

---

13 There are studies giving an approximate value to the GDP contributed by the ICT sector such as the "Índice País Digital" carried out by the País Digital Foundation and UDD, submitted in January 2015. This study estimated that the ICT sector represents 3% of the total Chilean economy (source from 2012). Likewise, in March 2015 the Under-Secretariat of Economy commissioned to F&K Consultores the study "Status of the Digital Development in Chile", which reported that the aggregate value of the ICT sector reaches 4.12% as compared with the total aggregated value (source from 2011).

14 Report "*Tecnologías de la Información y Comunicación en Chile: Áreas de investigación y capacidades, informe de estado del arte*" (Information and Communication Technology in Chile: Research Areas and Capabilities, State-of-the-art Report), Conicyt, 2010. "Índice País Digital", País Digital Foundation in conjunctions with UDD, January 2015. "Status of the Digital Development in Chile", F&K Consultores, March 2015.

15 Available in: http://www.agendaproductividad.cl/

7 Roles and required institutional structure to develop a national cybersecurity policy

A. Institutional structure for cybersecurity

It is essential for Chile, in order to fulfil this ambitious national cybersecurity policy and following the example of several other countries that have started this process some years ago, to have available a cybersecurity governance model responsible, at least, for carrying out such roles identified as essential -which are not being addressed, or are executed with no coordination within the country; therefore, the creation of an institutional framework to take up that role is hereby proposed.

A modern governance model and institutional framework which is in line with the needs of cyberspace and the country's digital development, will be a matter of law to be prepared and submitted by responsible institutional actors. Additionally, the creation of an advisory consulting council composed of different sectors will be assessed.

The roles identified as essential are: management of inter-institutional relationships, incident management, national and international point of contact, communications role, technical regulation and advisory role in general regulations, follow-up and evaluation of measures.

To carry out the above, correspondence of the cybersecurity framework with supplementary measures being developed in the area of digital governance within the State administration will be especially taken into account.

B. Transitional governance in cybersecurity

While the cybersecurity bill containing the final proposal for its institutional structure is discussed in the National Congress, certain essential roles identified up until now shall be temporarily performed by some of the institutions that are currently a part of the Government's structure.

An example of this is the role played by CSIRT Gob, which will be technically responsible for managing incidents arisen within the State's Connectivity Network, while, at a political level, it has been proposed to extend the term and scope of the Inter-Ministerial Cybersecurity Committee with regard to the communication, coordination and follow up roles of the different measures set out in the NCSP.

8 Public policy measures for 2017-2018

The measures below are an integral part of the public policy agenda to be implemented based on the strategic objectives described above[16].

	MEASURE	RESPONSIBLE - ASSISTING	OBJECTIVES NCSP
1	Prepare and forward to the National Congress a cybersecurity bill aimed at consolidating the institutional framework and incident management related with information security throughout the country.	MISP - MINDEF - MINHACIENDA - CICS (monitoring this measure)	A
2	Update Decree Law 83 about the State's information security aimed at the adoption of new standards and the creation of a model to control effective compliance.	MINSEGPRES	A
3	Add a cybersecurity dimension to the preparation and management of contracts for public concession tenders.	MOP (Concessions Department)	A
4	Create a working group responsible for developing a regulation and obligation framework for critical infrastructures in Chile, from a risk management focus.	MISP	A
5	Create a technical regulation for the development or contracting of software within the State, pursuant to standards for safe development.	MINSEGPRES	A
6	Create a platform to add information about cybersecurity incidents.	CSIRT	A
7	Coordinate the creation of updated requirements for regulated economic sectors	MTT - Super-intendence - CSIRT	A
8	Identify a minimum set of risks for Critical Information Infrastructure	CSIRT	A
9	Implement a standardised template for cybersecurity incident reports.	CSIRT, MINSEGPRES	A

16 The first body is the main responsible entity to carry out the task, and the other bodies support execution of the same. CSIRT means the current security equipment of the State's Connectivity Network, which will gradually take on operational duties identified in this policy.
Public institutions are identified with the following acronyms: CICS, *Comité Interministerial sobre Ciberseguridad* (Interministerial Committee on Cyber Securiry; MISP, *Ministerio del Interior y Seguridad Pública* (Interior and Public Security Ministry); MTT, *Ministerio de Transportes y Telecomunicaciones* (Transport and Telecommunications Ministry); MINDEF, *Ministerio de Defensa Nacional* (National Defence Ministry); MINHACIENDA, *Ministerio de Hacienda* (Finance Ministry); ANI, *Agencia Nacional de Inteligencia* (National Intelligence Bureau); MINJUSTICIA, *Ministerio de Justicia y Derechos Humanos* (Ministry of Justice and Human Rights); MINSEGPRES, *Ministerio Secretaría General de la Presidencia* (Ministry of the President's Office); MOP, *Ministerio de Obras Públicas* (Ministry of Public Works); MINEDUC. *Ministerio de Educación* (Ministry of Education); MINREL, *Ministerio de Relaciones Exteriores* (Ministry of Foreign Affairs); MSGG, *Ministerio Secretaría General de Gobierno* (Ministry of the Government's Office); MINECON, *Ministerio de Economía, Fomento y Turismo*, (Ministry the Economy, Development and Tourism).
When a ministry is mentioned without identifying a specific public service or under-secretariat, the reference relates with the under-secretariat participating in the Inter-Ministerial Committee on Cybersecurity or, should the corresponding ministry not be a part of the Committee, the corresponding ministry shall be responsible in general.

	MEASURE	RESPONSIBLE – ASSISTING	OBJECTIVES NCSP
10	Incorporate a cybersecurity dimension in the national emergency system.	MISP (CICS – monitoring this measure)	A
11	Prepare the regulation setting out safe mechanisms for exchanging information within the Government, between high level officers and other officials handling confidential or secret information.	MISP – MINDEF – ANI- MINREL- MINSEGPRES	A
12	Prepare a study about the resilience of telecommunication networks in Chile, proposing measures to improve it in the public and private fields.	MTT	A
13	Update the regulation on computer-related crimes.	MISP – MINJUSTICIA	B
14	Design and implement a standardised template to report cybercrimes.	MISP (with the police forces and ANI)	B
15	Promote the strengthening of investigation and forensic analysis skills related with cybercrime.	MISP (with ANI and the police forces)	B
16	Generate a first point for the dissemination of information to citizens based on the different digital channels and social networks enabled by the Internet.	MISP – MSGG (CICS – monitoring this measure)	C
17	Mark the Cybersecurity Month in October each year, promoting and developing activities to raise awareness at all levels. Additionally, participate in the Safe Internet Day in February.	MISP – MSGG (CICS – monitoring this measure)	C
18	Design and implement a large-scale cybersecurity campaign and promote the implementation of dissemination programmes in partnership with the private sector in awareness campaigns, with an emphasis on vulnerable sectors and a gender perspective.	MSGG (CICS – monitoring this measure)	C
19	Generate best practice guidelines both for citizens and the public sector.	CICS	C
20	Establish a cross-sectoral committee to promote cybersecurity at all levels and areas of the educational field.	MINEDUC- MINECON (Human Capital Committee) (CICS – monitoring this measure)	C
21	Design and implement a cybersecurity campaign aimed at the elderly population, including training and dissemination.	MDS (Senama) – MINECON (Human Capital Committee) (CICS – monitoring this measure)	C
22	Include Internet security issues in MINEDUC's specific programmes, promoting the ENLACES initiative.	MINEDUC (Enlaces) – MINECON (Human Capital Committee) (CICS – monitoring this measure)	C

	MEASURE	RESPONSIBLE – ASSISTING	OBJECTIVES NCSP
23	Strongly support the establishment, at an international level, of regional, sub-regional and multilateral political consultation processes, with special emphasis on the region.	MINREL	C
24	Advance the creation of bilateral work mechanisms, developing agendas and implementing cross-cutting political consultation instances with partner countries.	MINREL	D
25	Prepare a document containing Chile's international policy about cyberspace and cybersecurity.	MINREL - (CICS - monitoring this measure)	D
26	Establish an inter-agency working group to address international issued related with cyberspace.	MINREL - OTHER	D
27	Encourage the exchange of experiences with other countries in the field of cyber-security, with emphasis on the implementation and evaluation of strategies and policies.	MINREL	D
28	Analyse the regulation and application of the current system of public procurement supporting production and strategic domestic interests.	MINHACIENDA (Chilecompra Division) - MISP - MINDEF	D
29	Carry out studies both describing the cybersecurity industry (offer) and the use of cybersecurity in the country (demand), with the purpose of creating special programmes to promote the cybersecurity industry in specific sectors.	CORFO - MINDEF - MINECON	E
30	Analyse tax incentives, subsidies or R+D+I schemes in order to develop and adopt cybersecurity standards.	MINHACIENDA - MINECON - CORFO	E
31	Process the new law on personal data, conferring powers to a specific body that may impose security and notification requirements in connection with data leakage.	MINHACIENDA- MINECON	A, B
32	Develop one or more multi-sectoral cooperation opportunities with a series of social stakeholders (NGOs, companies, unions, and academia, *inter alia*).	CICS (committee coordinator)	A, B, C
33	Update Decree No. 5, 996 and Supreme Decree No. 1,299 in line with the amendments to Supreme Decree No. 83, setting out the requirements to access the network (self-assessment, online courses) and the obligation to report incidents by public bodies.	MISP	A, C
34	Carry out cyber exercises about cybersecurity incidents with different stakeholders in order to encourage the proper knowledge, research and dissemination of gaps, vulnerabilities and ways of mitigation in the national systems.	CSIRT	A, C

	MEASURE	RESPONSIBLE – ASSISTING	OBJECTIVES NCSP
35	Incorporate cybersecurity standards in the State's suppliers, requesting specific requirements for ICT suppliers, and analysing other requirements for other suppliers.	MINHACIENDA (Chilecompra Division)	A, E
36	Include a set of questions linked to cybercrime in the National Urban Survey on Citizen Security (ENUSC).	MISP (Under-Secretariat of Crime Prevention)	B, C
37	Prepare and regularly update a record of training offers for public servants about cybersecurity available in international organisations and national institutions.	MISP - MINREL	B, C, D
38	Adhere to and implement the Convention on Cybercrime of the Council of Europe.	MISP - MINREL - MINJUSTICIA- OFFICE OF THE PROSECUTOR	B, D
39	Encourage State support of R+D+I projects with public or private financing, whether national or international, in the field of cybersecurity.	CICS	C, E
40	Promote the development of advanced human capital regarding cybersecurity in the different technical-professional or vocational areas.	CORFO - MINECON (Human Capital Committee)	C, E
41	Support the export of national products and services in the field of cybersecurity, identifying international exhibitions and evaluating support actions.	MINREL (Prochile) - MINECON	D, E

9 Annexes

Annex No 1: Standards and institutions involved in cybersecurity in Chile

1. RELEVANT STANDARDS AT A NATIONAL LEVEL

a. Political Constitution of the Republic of Chile

- **Article 8,** about public transparency
- **Article 19**, including a catalogue of fundamental rights, with the most relevant ones being: **No. 2**, equality before the law; **Nos. 3 and 7**, due process and individual safety; **Nos. 4 and 5**; protection of life and inviolability of communications; **No. 12**, freedom of speech and freedom of information, and **Nos. 24 and 25**, property and freedom of creation.
- **Article 24**, vesting upon the person who acts as President of the Republic the authority to safeguard the public order in and the external security of the Republic, apart from the regulations that govern the authorities vested upon other State powers and bodies.
- **Articles 39 and following** regulating specific **situations** that affect the normal operation of the State.

b. Laws

- **Criminal Procedure Code:** This piece of legislation regulates criminal investigation and prosecution in Chile, and, within this framework, any investigation related with cybercrime that may be carried out in the country. Additionally, it regulates a set of intrusive measures that may affect the recipient's private life or inviolability of communications and, therefore, the inviolability of their communication –for which purpose the Law demands certain legal requirements and a court order authorising the practice of such measures.
- **Law No. 19,913, which creates the financial analysis unit and modifies a series of provisions in the field of money laundering and bleaching:** This law regulates some investigation and surveillance measures that, as in the case of the Criminal Procedure Code, may affect the recipient's private life or inviolability of communication and, therefore, the confidentiality of their information –for which reason the Law in this case also requires a court order in conjunction with the fulfilment of the legal requirements of the case.
- **Decree Law No. 211, Free Competition Law:** As in the previous case, this law authorises the carrying out of intrusive in specific cases and in the same terms described above.
- **Law No. 19,974, about the System of the State's Intelligence and creating the National Intelligence Bureau:** Within the framework of intelligence information gathering, this Law regulates the practice of special procedures to gather information, which has to be done under a court order and taking into account a series of legal safeguards restricting the gathering and use of this information.

- **Criminal Code:** This legal piece is the country's main criminal catalogue containing the description of a set of specific conducts together, with the associated sentences. Regarding cybersecurity, this code describes a series of conducts that may be carried out through cyberspace or affects the elements thereof, having a key relevance in the development of policies and the combat against cybercrime.
- **Code of Military Justice:** A legal piece containing specific provisions regarding crimes mostly perpetrated by members of the armed forces or at times of war. The provisions of this legal piece cover crimes related with espionage and disclosure of certified information to third parties, with the purpose of protecting the national security.
- **Law No. 19,223** There is a sub-category in the field of cybercrime related with the disturbance of the logical components of cyberspace (computer programmes, information systems, databases) called computer-related crimes. This Law sets out specific criminal definitions describing the non-authorised access, theft and destruction of information systems.
- **Law No. 20,009 covering the Loss, Theft or Robbery of Credit and Debit Cards.**
- **Law No. 18,168, General Telecommunications Law:** This piece of legislation regulates the legal framework of the country's telecommunication industry which provides key physical and logical infrastructure for the national cyber space. One of its provisions set out the protection, confidentiality and integrity of the information through the criminalisation of offences related with the non-authorised interception (art. No. 36B, letters b and c). Two recent modifications are especially relevant for the country's cybersecurity, namely: **Law No. 20,453 that ensures the principle of network's neutrality for Internet consumers and users,** regulating network management measures that may be adopted by Internet service providers and ensuring the duty of confidentiality, and **Law No. 20,478, about business recovery and continuity when the public telecommunications system is affected by critical and emergency situations,** enacted after the earthquake that affected the country in 2010. As described by its name, this Law sets out a set of measures allowing maintaining the continuity of the country's telecommunications and, therefore, the availability of information contained in the cyberspace.
- **Law No. 19,799 regarding electronic documents, electronic signature and signature certification services:** This Law regulates the use of electronic documents in the country, with the corresponding mechanisms to ensure information integrity and confidentiality by the use of digital signature, together with a system guaranteeing the proper operations of the bodies providing this service.
- **Law No. 20,285 about the access to public information:** This piece of legislation creates a transparency scheme for the State's activities, with active transparency obligations, which must be carried out through the website of each relevant public body; and passive obligations, which consist in providing the data that any person may require from these bodies, provided that this does not affect other rights and interests set out in the law -such as the State's security and third party's privacy, so that the confidentiality of the relevant is not affected.
- **Law No. 19,628 regarding the protection of private life:** This law sets out a series of principles and rights relative to the management of personal data in the country that may be requested by the owner of the personal data to whom is in possession of or manages a record containing such data, together with the general application rules for the management of personal data by the public and private sectors in connection with the safeguarding of the data contained in such information.

c. Decrees

- **Supreme Decree No. 83/2005 approving the technical regulations for the State administration bodies about the security and confidentiality of electronic documents:** This decree, which evolves from the provisions contained in Law No. 19,799, sets out a regulation for the public administration of the State about the security and confidentiality of electronic documents, together with the information infrastructure based on ISO standard 27,000, with the setting out of administrative measures such as the creation of information security committees in each public service. This decree is supplemented with **Supreme Decree No. 93/2006 that approves the technical regulation for adopting measures aimed at minimising the detrimental effects of unwanted spam messages received in the mailboxes of the State administration bodies and their officers.** As described, this decree sets out the measured aimed at preventing spam from being received by the State's administration bodies.
- **Supreme Decree No. 1,299/2004 setting out new regulations for the State's Connectivity Network managed by the Ministry of the Interior and describing the technological procedures, requirements and standards for the incorporation to such network by public bodies:** This decree, based on the provisions of the 2005 budget law, and Supreme Decree No. 5,996/1999, consolidates an intranet, named the State's Connectivity Network, where a number of ministries and public bodies should be interconnected. Centralising Internet access, this network has to comply with security technical standards in line with IEEE and ISO standards.
- **Supreme Decree No. 1/2015 approving the technical standards for the systems and websites of the State administration bodies:** This Decree updates the technical standards for the websites of the State administration bodies regulating certain conditions about confidentiality, availability and accessibility of information contained in those websites, all of them being key elements of cybersecurity.
- **Supreme Decree No. 533/2015 that creates a Cybersecurity Inter-Ministerial Committee:** This decree creates an Inter-Ministerial Committee responsible for developing a proposal for the National Cybersecurity Policy, of which this Annex is an integral part.

2. INSTITUTIONS INVOLVED IN THE FIELD OF CYBERSECURITY

a. Ministry of the Interior and Public Security

Body	Role	Mission
Undersecretary of the Interior	Preventive Public policy design	The mission of the Ministry of the Interior and Public Security is to safeguard public security, coordinating, evaluating and monitoring the execution of inter-sectoral plans in the field of crime prevention and control (Art.1, Law No. 20,502), including cybercrime, and to design public policies in order to prevent, challenge and punish the same. In particular, the Organised Crime Department is responsible for developing strategies for combating cybercrime (Exempt Resolution No. 10,168, 3/12/2013).
Undersecretary of the Interior	Preventive Reactive Public policy design	By virtue of Decree No. 5,996 of 1999, the MISP is responsible for implementing and operating, at a national level through the Computer Division, the State's Connectivity Network (RCE). Supplementing the decree mentioned above, Supreme Decree No. 1,299 of 2004, grants this State body the power to publish or disseminate the country's official regulations in the field of information security and to set out logic security regulations, standards and policies that public bodies included in the RCE shall be obliged to fulfil. This division was also granted the power to submit technical consultations to any State body. It is worth mentioning the RCE's role as a tool to support Government cybersecurity.
Investigations Policy (PDI), Cybercrime Investigation Brigade	Preventive and investigative	This Brigade is responsible for investigating crime under the direction of the Office of the Prosecutor, including cybercrime.
***Carabineros* Police, OS9 Department**	Preventive and investigative	According to Law No. 19,974 regulating this Department's responsibilities, one of its duties is to: "propose regulations and procedures to protect the State's critical information systems", Art. 8, letter c).

b. Ministry of National Defence

Body	Role	Mission
Defence Under-Secretariat	Policy design	The Defence Under-Secretariat is responsible for developing and updating the relevant primary planning and policies to face the challenges of cybersecurity for the National Defence, and ensuring that it is in line with the secondary planning thereof.
Joint Staff of the Armed Forces	Preventive and reactive	The Armed Forces are responsible for protecting their own information infrastructure. Additionally, they cooperate in tasks related with the national cybersecurity and national intelligence systems. The Joint Staff is the Ministry of Defence's permanent working and advisory body in matters having a connection with the joint preparation and use of the Armed Forces, thus being responsible for preparing and updating the Defence's secondary planning, together with other tasks relevant for the country's cybersecurity. The Armed Forces, pursuant to the planning carried out, are responsible for executing the relevant institutional and operational plans.

c. Ministry of Transport and Telecommunications

In charge of designing public policy and monitoring compliance in the area of telecommunications, the Telecommunications Under-Secretariat is also responsible for the implementation of Law No. 20,478 about "Business Recovery and Continuity under Critical and Emergency Situation of the System of Public Telecommunications", which task is executed through Decree No. 60/2012 setting out the Regulations for the inter-operation and dissemination or alert messages, the declaration and safeguarding of the telecommunications' critical infrastructure, and the information regarding serious failures of the telecommunications systems. Likewise, this Under-Secretariat is responsible for monitoring the respect for the principle of the network's neutrality set out in Law No. 20,453.

d. Ministry of Economy, Development and Tourism

This Ministry is responsible for designing public policies for encouraging productivity. The Ministry of Economy's mission is promoting the modernisation and competitiveness of the country's productive structure, the private initiative, and the market's efficient action, as well as the advance of innovation and the consolidation of the country's economy at an international level; therefore, cybersecurity as a focus for national development is included in the Productivity, Innovation and Growth Agenda.

e. Ministry of Justice and Human Rights

Pursuant to its role in the modernisation of the justice system, as well as in the development of regulations and policies aimed at facilitating the access to and protection of people's fundamental rights and citizen security, the Ministry of Justice and Human Rights is responsible for seeing to the ongoing updating and technical adequacy of legislation to the challenges posed by technological development.

f. Ministry of Foreign Affairs

Performing an articulation role within the international community and responsible for the international coordination of the national cybersecurity policy, the Ministry's *Dirección de Seguridad Internacional y Humana* (Department for International and Human Security), (DISIN), is responsible for identifying, coordinating and promoting Chile's cybersecurity position and interests within the international community, in all its dimensions. Likewise, the Ministry coordinates and promotes Chile's involvement in specialised international bodies and forums (Meridian, Octopus, OAS, UNASUR, ITU, IGF, UN expert groups, *inter alia*). It is also responsible for promoting bilateral relations in this field.

g. Ministry of the President's Office

With regard to the design of public policy in the area of digital government and digital development, the purpose of the Ministry of the President's Office, through the State Modernisation Unit, is to make the State accessible for people, with the relevant modernisation of the State and digital Government.

h. University of Chile

Body	Role	Mission
NIC Chile	Technical body, administrator	NIC Chile is the organisation responsible for the names containing the .CL domain, and for operating the technology allowing the efficient and safe operation of these names, so that people, companies and institutions may be identified in the Internet.
CLCert	Academic body, contact point with international CERTs and FIRST	CLCert's main objectives are: -Provide, in a timely and systematic fashion, information about security vulnerabilities and threats. -Disseminate, and make available to the community, information allowing the prevention and solution of this type of security incidents. -Educate the general public about security matters, promoting policies allowing implementation thereof

i. National Standards Institute (*Instituto Nacional de Normalización*)

A technical body responsible for setting out standards and accreditations, the National Standards Institute (INN) is a private law, non-for-profit foundation created by CORFO in 1973 as a technical body in charge of overseeing quality infrastructure which, in the cybersecurity fields, relates with a series of ISO/IEC 27000 standards.

j. Office of the Prosecutor

Exercising its role to lead the criminal prosecution process and carry out the public criminal action, the Office of the Prosecutor is an autonomous body responsible for investigating criminal offences, taking the accused before the courts and, if relevant, providing protection to victims and witnesses leading.

k. Judicial Branch

The Judiciary, which has the exclusive power of hearing, resolving and executing sentences in civil and criminal lawsuits, is composed of courts having different competences, namely, civil, criminal, labour and family courts. With regard to cybersecurity, judges have the power to order some intrusive actions, control the legality of criminal investigations, and decide upon criminal cases, including cybercrime.

Annex No 2: Risk and threat overview

1. SOURCES AND TYPES OF RISKS AND THREATS

Due to the global nature of cyberspace, risks come from threats both from Chile and abroad and have different origins relevant for the country, namely:

- **Internal incidents:** Involuntary information leakages, accidental interruption of information systems, or other involuntary incidents that may affect the confidentiality, integrity, availability and traceability of the information.
- **Natural disasters or *force majeure:*** Earthquakes, floods and other disasters that may affect cyberspace caused by the destruction of physical infrastructures essential for information availability.
- **Espionage and surveillance activities carried out by State actors:** Conducts that affect information confidentiality due to theft of the same for political or strategic purposes. Particularly important is the use of sophisticated tools known as APT (Advanced Persistent Threat) that, in turn, may benefit from non-published computer vulnerabilities of technologies in use.
- **Denial of Service and Distributed Denial of Service (DOS and DDOS) attacks:** These attacks relate with the intentional overcharge of services provided in a computer system which, in turn, can be conducted from one point of the network, or distributed to coordinate the attack from various points, many times by using infected devices with malicious programmes in order to achieve their objective.
- **Cybercrime:** Criminal activities perpetrated against components in the cyberspace (non-authorised access, information sabotage, information theft, information hijacking or ransomware) or employing tools in cyberspace as a means for such crimes (phishing, pharming, virtual fraud, and other related crimes).
- **Attacks against critical infrastructures through the cyberspace:** An alteration in the operation of critical infrastructures (both physical and information infrastructure) carried out by electronic means, e.g. the large-scale disruption of financial systems, interference of basis services, physical damage to physical structures and other related attacks.

All the above risks and threats affect the confidentiality, integrity, availability and traceability of information assets in the cyberspace and, in the medium-term this may affect the country's development in cyberspace, thus depriving us from the benefits associated with the digital government, ways of social organisation facilitated by cyberspace and threats to the security of people and institutions in this field. Some cases may fit in more categories than the ones described herein.

2. RISKS AND THREATS IN THE GLOBAL CONTEXT

At a global scale, there are many examples of cyber attacks consisting in espionage activities and distributed denial of service (DDoS) attacks in the Internet. Likewise, the large-scale interception of telecommunication networks, the failure of Internet services, espionage activities against governments and companies, as well as attacks against critical infrastructures such as banks and Government services, have been regularly in the news. There is also plenty of evidence with regard to legal abuses in the request for data to diverse providers of digital goods and services by countries where such providers are based.

Some cases worth mentioning are: Iran (2010), whose nuclear centrifuges were disabled by a computer virus especially designed for such purpose; Estonia (2007), where part of its critical infrastructure was disabled for weeks; disclosures by Edward Snowden (2013) about widespread espionage activities by the United State's intelligence agencies –which scope is still undetermined due to the number and regularity of such disclosures; and espionage activities against companies in the defence field (Lockheed, 2011) and entertainment (Sony, 2014),also in the US, which scope seriously compromises the economic interests and fundamental rights of people around the world.

3. RISKS AND THREATS IN A REGIONAL CONTEXT

Regionally, the countries that have reported the highest number of cyber attacks in Latin America were Brazil, Argentina, Colombia, Mexico and Chile. Accesses and information theft from infected computers – called *botnets* – were widespread in the region. There was even a specific type of malicious code called *dorkbot* that generated over 80K actions against the virtual system, with higher concentrations in Chile (44%), Peru (15%) and Argentina (11%)[17].

4. MALICIOUS ACTIVITIES DETECTED IN THE STATE'S CONNECTIVITY NETWORK

In Chile, the State's Connectivity Network (RCE) is affected by many malicious or suspicious activities. There is an incident record related with distributed denial of service (DDoS) attacks or alterations in Government website's operations, with an increasing number of these incidents starting in 2010. Likewise, in 2015, at a general level, administrators of the Government network spotted the following patters:

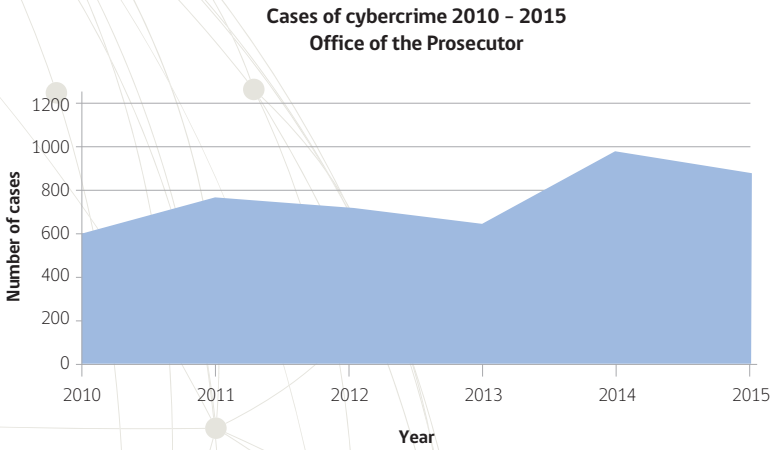
17 Prandini, P. & Maggiore, M. 2013. Op. Cit.

Number of Records	Description
58375435	Attempts to access information in network devices through SNMP protocol.
45903511	Scanning of device administration ports in switch, router or security platforms.
19745086	Web flow with password transfer in clear text (no encryption).
7805544	Detection of DNS dynamic updates.
5570661	Detection of TFTP flow (file transfer) by using tftp protocol.
4463394	Detection of portmap flows.
3359194	Detection of anomalous traffic in DNS ports.
2479277	Detection of remote desktop flows.
2077435	Detection of DNS queries by domains recognised as using malware.
2023403	Detection of recognition by PING.
1451708	Scanning of device administration ports in switch, router or security platforms.
1428461	Detection of wordpress access (key components).
1400697	Detection of MORTO malware.
1120311	Detection of NON encrypted traffic through a port usually used to transmit encrypted traffic (443).
1106303	Detection of access to forbidden areas in websites.
1025252	Flow of credentials in clear text of wordpress login (used in Government websites).

Patterns detected in the State's Connectivity Network (RCE) in 2015.
(Source: IT Division of the Ministry of the Interior, 2016).

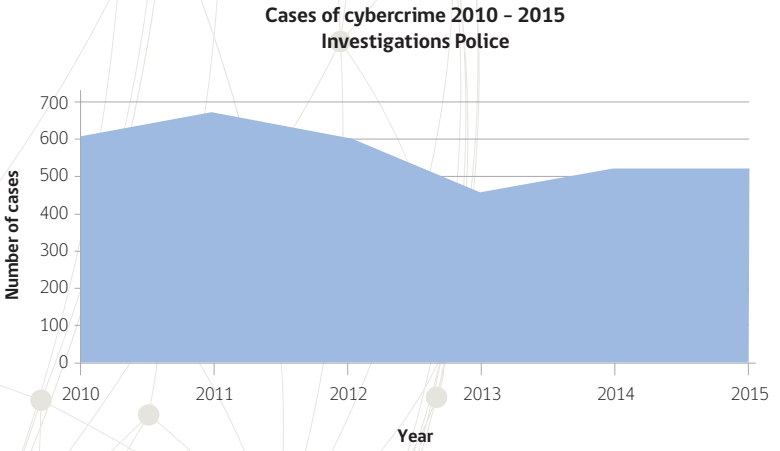
5. CYBERCRIME IN CHILE

According to figures provided by the Office of the Prosecutor, regarding cybercrime between 2010 and 2015, the number of cases submitted with the name "computer-related crime" was 4,648 cases, distributed as described below:



Cases submitted as cybercrime in 2010-2015 by the Office of the Prosecutor, related only with the types of offences set out in Law No. 19,233 (Source: ULDDECO, Office of the Prosecutor, 2016[18]).

Likewise, according to the data provided by the Investigations Police (PDI), during 2010-2015, a total number of 3,370 investigations distributed as described below:



Number of cybercrime investigations carried out in 2010-2015 by the PDI (Source: Cybercrime Brigade, PDI, 2016).

The *Carabineros* Police, on their part, have identified different types of illicit behaviour in the cyberspace at a national level, the most common ones being the fraudulent access to systems; the purchase, sale and storage of child pornography; computer sabotage, and illicit banking operations (phishing).

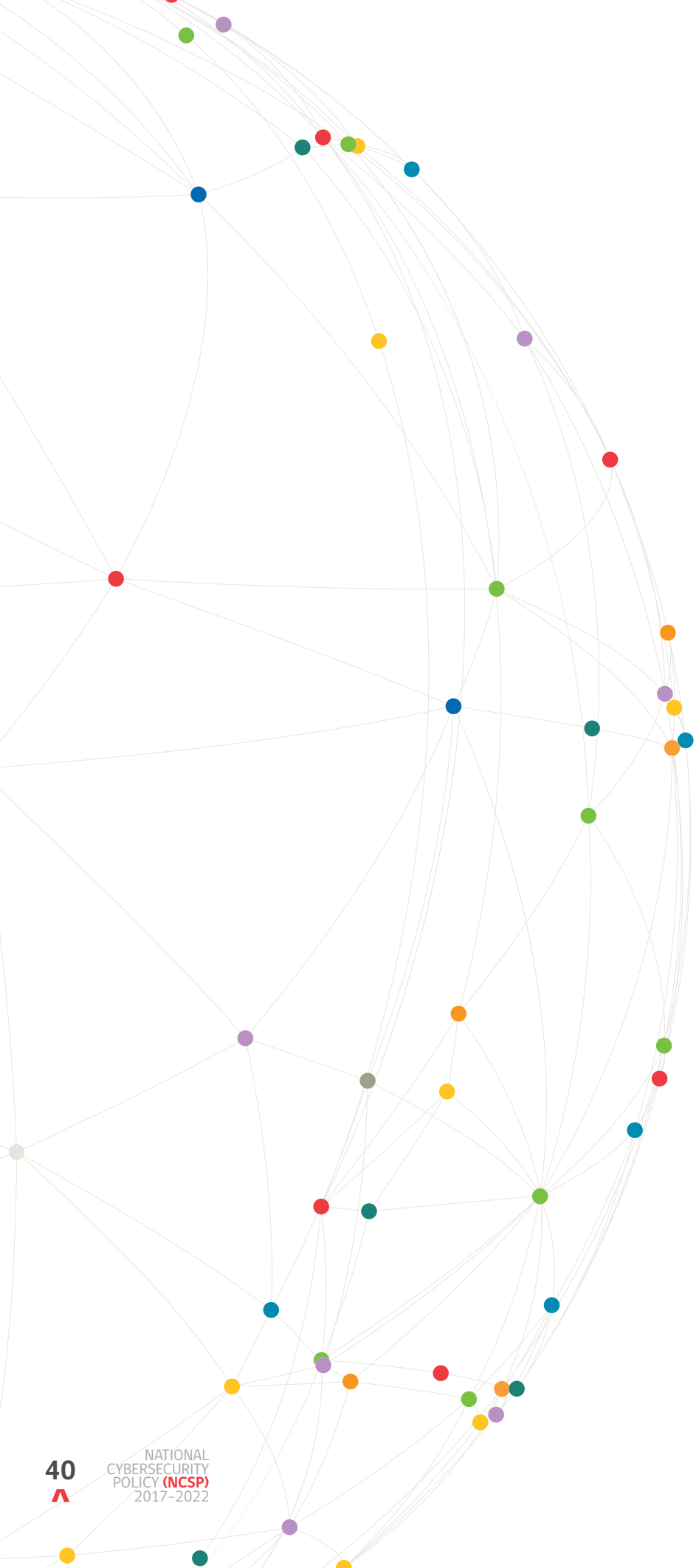
18 Chilean Office of the Prosecutor. A brief description of the current state of regulations and sentences in Chile regarding cybercrime. Specialised Unit for Investigating Money Laundering, Economic Crimes, Environmental Crimes and Organised Crime. As stated in the document mentioned, data presented are not the real total number of the cases as many of them are reported as fraud (Page 6).

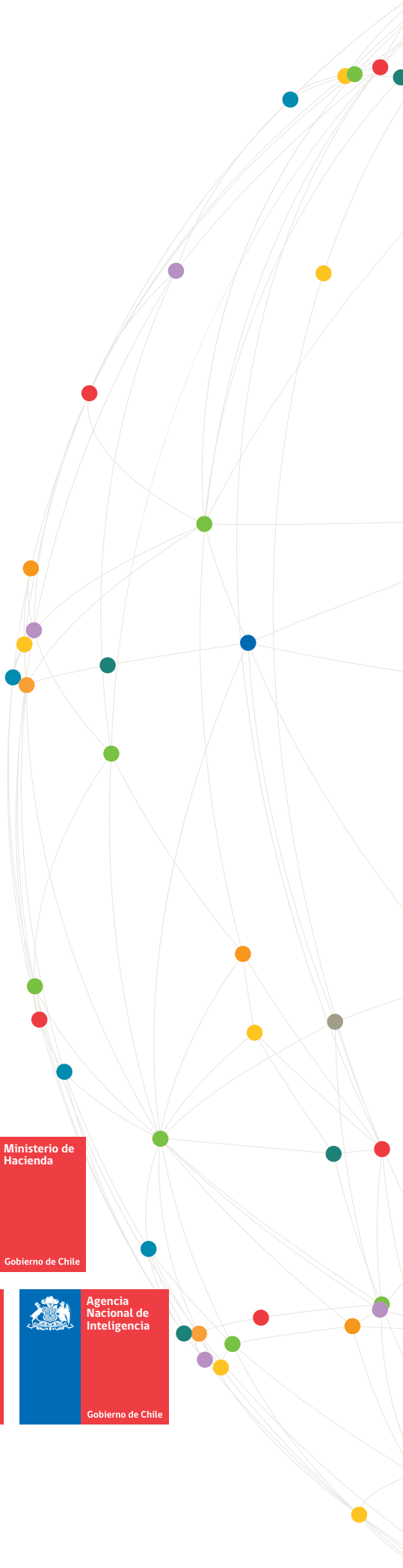
Likewise, cybercrime perpetrated in Chile confirm the cross-border nature of illicit acts in the cyberspace, specifically regarding the fraudulent use of credit and debit cards, where people from different nationalities have been found to plan and perpetrate such crimes.

Conclusion

The information contained in this document represent a threat for the confidentiality, integrity, availability and traceability of information in the cyberspace, which affects all users and deprives them from using cyberspace in a safe fashion, violating state and trade secrets and threatening people's fundamental rights, especially the rights connected with the protection of private life and communication inviolability.

For the reasons described above, it is essential to have policies in place to manage and minimize risks take into account such risks and threats, especially with regard to critical information infrastructure, with proper consideration of the special regulation set out for the purchase and operation of technological solutions and taking into account the international context in the field of cybersecurity.





CICS Comité Interministerial sobre Ciberseguridad

www.ciberseguridad.gob.cl

Subsecretaría del Interior
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Ministerio de Relaciones Exteriores
Gobierno de Chile

Subsecretaría de Defensa
Gobierno de Chile

Ministerio de Hacienda
Gobierno de Chile

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

Ministerio de Economía, Fomento y Turismo
Gobierno de Chile

Ministerio de Justicia y Derechos Humanos
Gobierno de Chile

Subsecretaría de Telecomunicaciones
Gobierno de Chile

Agencia Nacional de Inteligencia
Gobierno de Chile