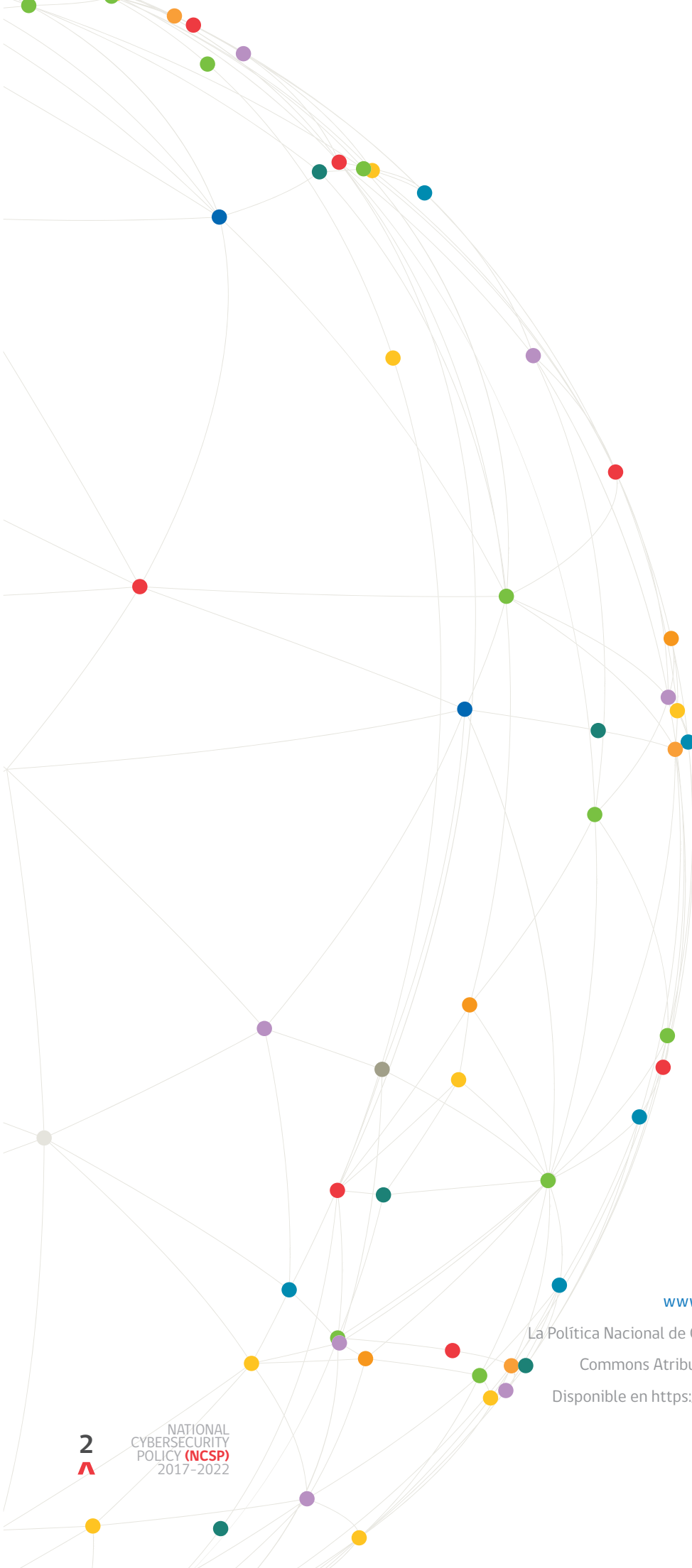




POLÍTICA NACIONAL DE CIBERSEGURIDAD





www.ciberseguridad.gob.cl

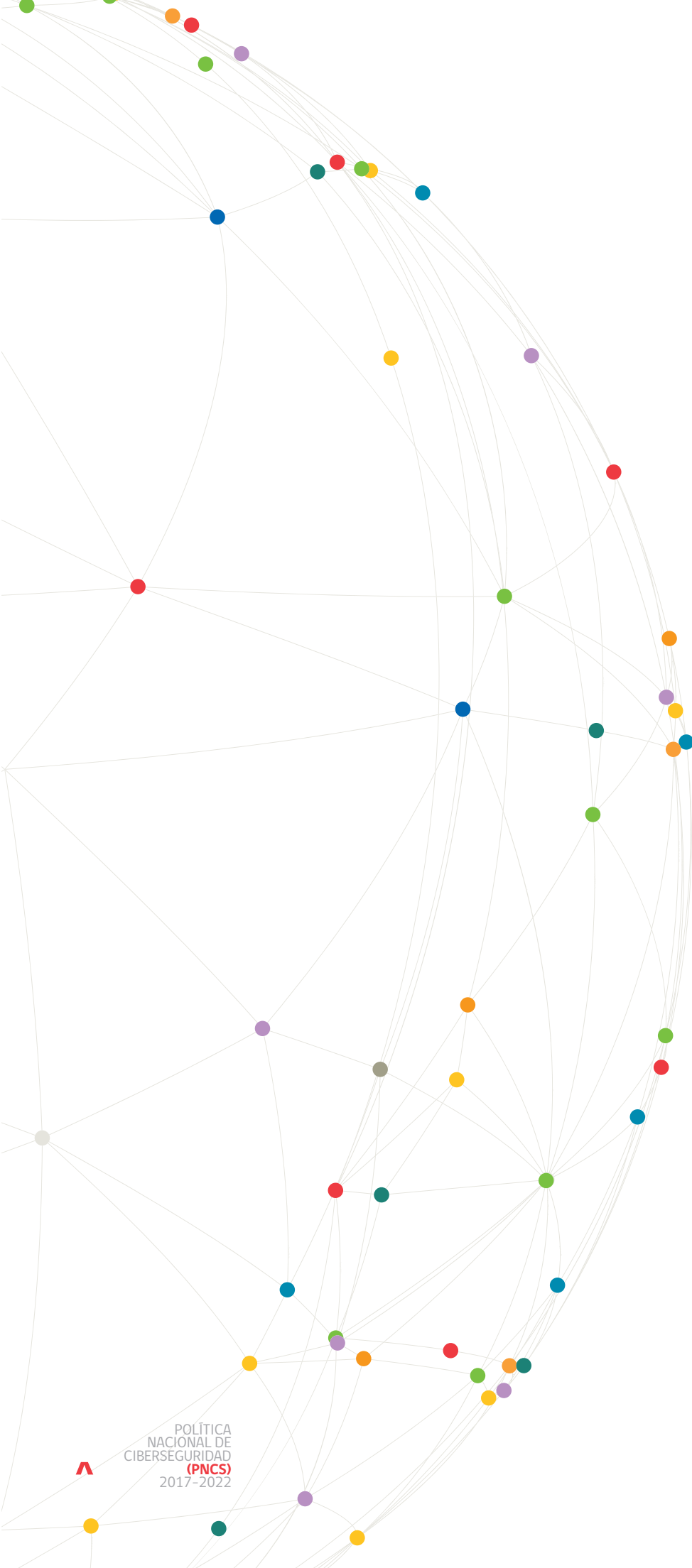
La Política Nacional de Ciberseguridad está bajo una Licencia Creative Commons Atribución-CompartirIgual 4.0 Internacional.
Disponible en <https://creativecommons.org/licenses/by-sa/4.0/>

2
A

NATIONAL
CYBERSECURITY
POLICY (NCSP)
2017-2022

Índice

>	1. Introducción	5
>	2. ¿Por qué se requiere una política nacional de ciberseguridad?	6
>	3. Estado actual de la ciberseguridad: normas, instituciones, panorama de riesgos	7
>	4. Hoja de ruta de la política	8
>	5. Objetivos de política para el año 2022	10
>	6. Funciones e institucionalidad necesarias para desarrollar una política nacional de ciberseguridad	19
>	7. Medidas de política pública 2017-2018	20
>	8. Anexos	24
	Anexo N° 1: Normas e instituciones que intervienen en ciberseguridad en Chile	24
	Anexo N° 2: Panorama de riesgos y amenazas	30



POLÍTICA
NACIONAL DE
CIBERSEGURIDAD
(PNCS)
2017-2022



1 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 ciberseguridad¹, 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 2022³, 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.



2 ¿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.

3 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 N° 19.223 sobre delitos informáticos o la ley N° 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 región⁶.

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 N°1 con detalle de la normativa e institucionalidad existente en materia de ciberseguridad.

5 Ver anexo N°2 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.



4 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 2020⁷ 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 N°11 de la Agenda Digital 2020, que apunta a generar una visión país sobre gobernanza de internet.



5 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 Europa⁸, 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 físico⁹. 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 otros¹².

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 países¹³, 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 alternativa¹⁴. 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 Crecimiento¹⁵ 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/>

6 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.



7 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 anteriormente¹⁶.

 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





8 Anexos

Anexo N°1: Normas e instituciones que intervienen en ciberseguridad en Chile

1. NORMAS RELEVANTES A NIVEL NACIONAL

a. Constitución Política de la República

- **Artículo 8°**, relativo a la transparencia pública.
- **Artículo 19°**, que contempla un catálogo de derechos fundamentales donde son especialmente relevantes: N°2, igualdad ante la ley; **N°3 y 7**, relativos al debido proceso y seguridad individual; **N°4 y 5**, sobre protección de la vida privada e inviolabilidad de las comunicaciones; **N°12**, que garantiza la libertad de expresión y de información; y **N°24 y 25**, relativos a la propiedad y libertad de creación.
- **Artículo 24°**, 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 39° 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 N°19.913, 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. N° 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 N°19.974, 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 N°19.223, 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 N° 20.009 sobre Extravío, Robo o Hurto de Tarjetas de crédito y débito**
- **Ley N° 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. N°36B letras b y c). Cobran también especial relevancia para la ciberseguridad del país dos modificaciones recientes, correspondientes a la **Ley N°20.453, 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 N°20.478, 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 N°19.799, 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 N°20.285, 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 N°19.628, 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. N°83/2005, 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 N°19.799, 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. N°1.299/2004, 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. N°1/2015, 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. N°533/2015, 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.

2. INSTITUCIONES INTERVINIENTES EN MATERIA DE CIBERSEGURIDAD



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	<p>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.</p> <p>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.</p> <p>Las Fuerzas Armadas, por su parte, están a cargo, acorde a la planificación realizada, de los planes institucionales y operativos que correspondan.</p>

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 N°2: 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: interrupción 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 entretenimiento (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.



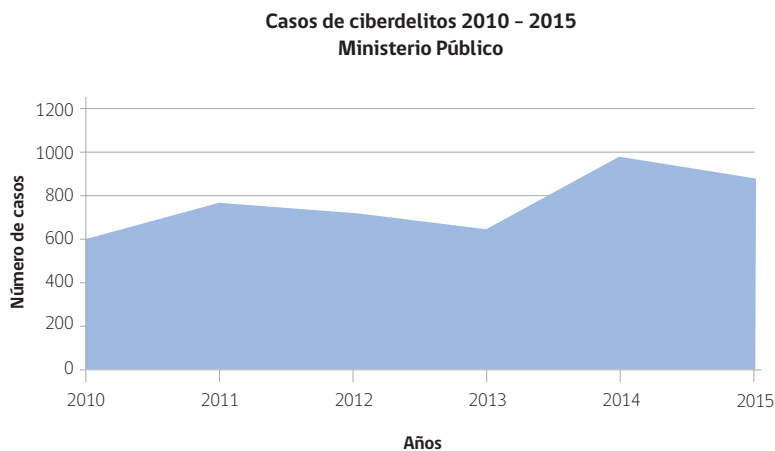
Cantidad de Registros	Descripción
58.375.435	Intentos de acceder a información de dispositivos de red mediante protocolo de administración SNMP
45.903.511	Escaneo de puertos de administración de dispositivos de la plataforma switch, router o seguridad.
19.745.086	Flujo web con traspaso de contraseñas 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 tráfico 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)



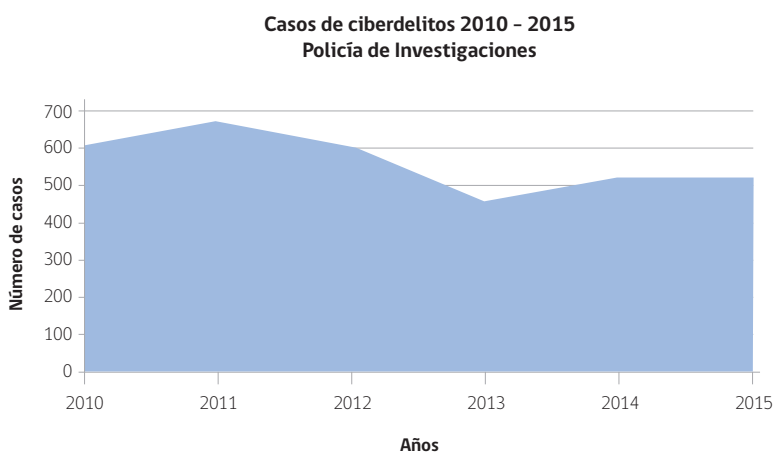
5. CIBERDELITOS EN CHILE

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 cibercrimitos 2010 – 2015 por Ministerio Público, referidos sólo a las figuras reguladas en la Ley N°19.223 (Fuente: ULDDECO, Ministerio Público, 2016¹⁸).

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 cibercrimitos 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 Cibercrimitos. 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).



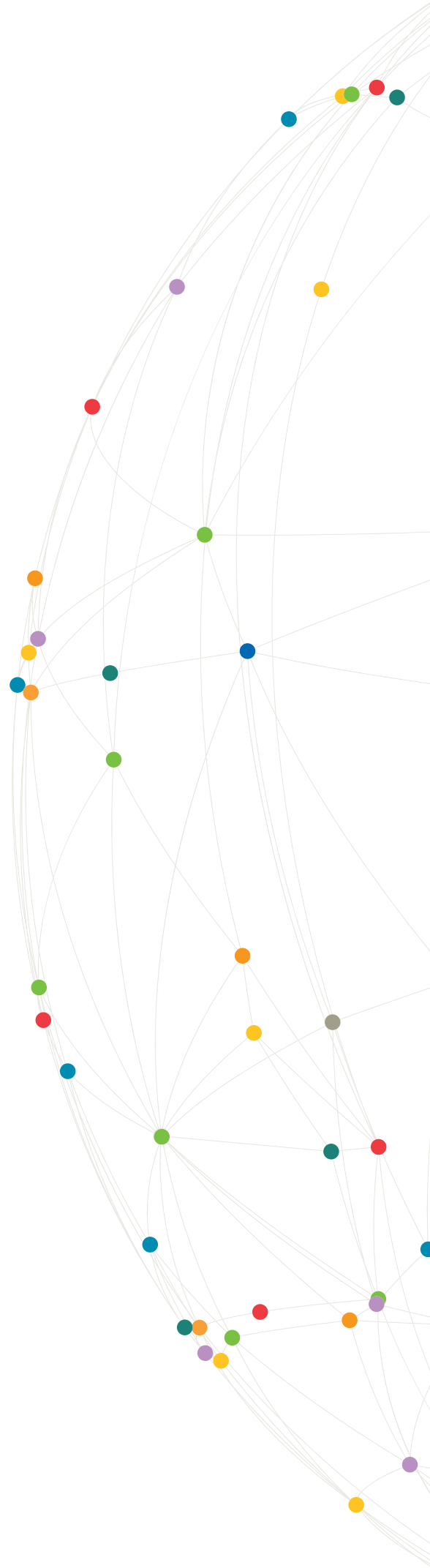
Por su parte, Carabineros identifica diferentes tipos de ilícitos en el ciberespacio a nivel nacional, siendo los más comunes el acceso indebido a sistemas; la adquisición, comercialización y almacenamiento de material pornográfico infantil; sabotaje informático; y transacciones bancarias ilícitas (*phishing*).

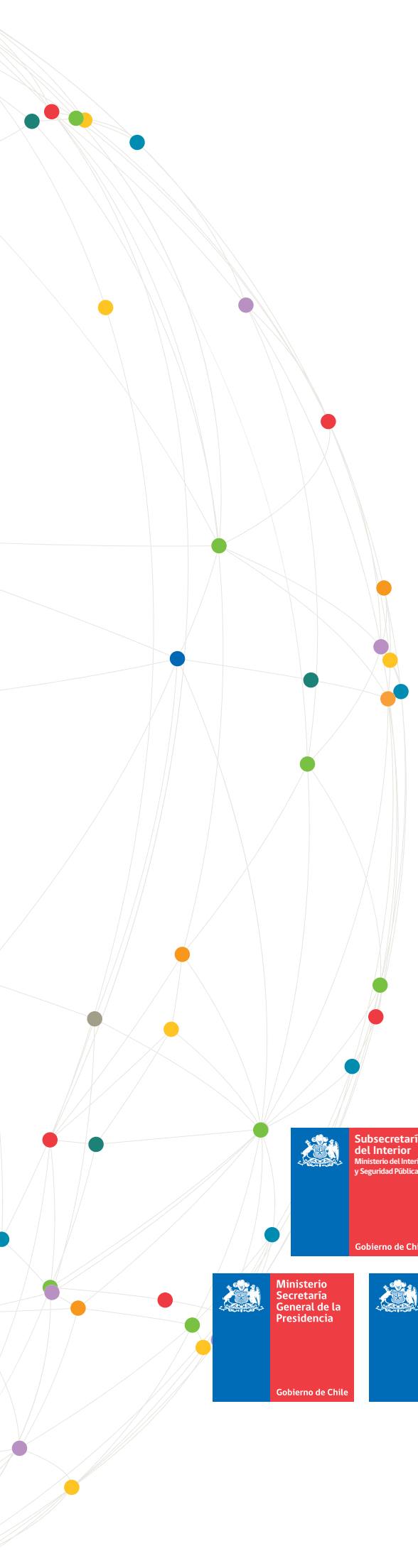
Asimismo, los cibercrímenes cometidos en Chile confirman el carácter transnacional de los ilícitos en el ciberespacio, específicamente, en el uso fraudulento de tarjetas de crédito y débito, con la detección de personas de diferentes nacionalidades, en la planificación y comisión de dichos delitos.

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

