La participación en la elaboración de la

POLÍTICA NACIONAL DE CIBERSEGURIDAD:

HACIA UN NUEVO MARCO NORMATIVO EN CHILE

La participación en la elaboración de la

POLÍTICA NACIONAL DE CIBERSEGURIDAD:

HACIA UN NUEVO MARCO NORMATIVO EN CHILE

Pablo Viollier

Pablo Viollier

El autor agradece la colaboración de Constanza Canales Loebel
en el proceso de revisión de los comentarios y su sistematización.

PORTADA: *Harol Bustos*
DISEÑO: *Cristóbal Correa*
EDICIÓN Y CORRECCIONES: *Vladimir Garay y Patricio Velasco.*
Octubre 2017.

Este informe fue realizado por Derechos Digitalesen conjunto con Global Partners Digital y financiado por el Ministry of Foreign Affairs de los Países Bajos.

Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005 y cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital, desde el interés público. Entre sus principales ejes de interés está la defensa y promoción la libertad de expresión, el acceso a la cultura y la privacidad.

CONTENIDOS

1. INTRODUCCIÓN

La ciberseguridad ha adquirido una relevancia cada vez mayor en las agendas de los gobiernos y los actores privados, pasando de ser un tema de exclusiva incumbencia de los técnicos del área de la informática, a un foco de política pública en donde intervienen académicos, empresas, periodistas, políticos y miembros de la sociedad civil.

Los ataques informáticos de gran escala, cada vez más sofisticados y frecuentes, han transformado a la ciberseguridad en un tema de interés para la opinión pública, prioritario para el mantenimiento del modelo de negocios de las empresas que dependen de la red y de relevancia estratégica para los gobiernos.

Chile no ha estado exento de esta tendencia. Nuestro país ha sufrido distintos ataques informáticos de escala mundial: cuando en mayo de 2017 se desencadenó una serie de ataques de *ransomware*, en nuestro país se detectaron al menos 270 casos de equipos afectados.[1] La comisión de delitos informáticos en el país también ha generado debate; de acuerdo a cifras de la Subsecretaría del Interior, durante el primer semestre de este año se reportaron 23.928 ciberdelitos. De estos, solo 517 son delitos informáticos propiamente tal, es decir, los tipificados por la Ley 19.223. Los 23.411 restantes corresponden a uso indebido de tarjetas de crédito y débito (La Tercera, 2017).

Por otro lado, las revelaciones de espionaje gubernamental masivo, como el revelado por Edward Snowden en junio de 2013, han ayudado a generar un consenso cada vez mayor respecto a la necesidad de un internet abierto, democrático y seguro para el correcto desarrollo de la libertad de expresión, la economía, el consumo de bienes culturales y el intercambio de ideas.

De lo anterior se deduce la necesidad de contar con políticas nacionales que permitan coordinar y generar una hoja de ruta clara para el diseño, implementación y puesta en marcha de medidas que permitan proteger la seguridad y los derechos de los usuarios en el ciberespacio.

Para ello es necesario analizar las características propias de nuestro país por que determina los desafíos específicos que debemos enfrentar en materias de ciberseguridad. En ese sentido, un aspecto a considerar es, por ejemplo, la geografía: al ser Chile un país largo y angosto, es menos costoso extender un único trazado de fibra óptica de norte a sur, haciendo más dificultoso poder asegurar la redundancia de la red, la interconexión de proveedores y la existencia de acuerdos de ruteo en caso de emergencias (José Miguel Piquer, 2015).

A fin de enfrentar estos y otros desafíos de forma coordinada y sistemática, el gobierno de Chile emprendió la elaboración de una Política Nacional de Ciberseguridad (desde ahora, PNCS). Luego de un proceso de deliberación entre agencias del gobierno, que incluyó audiencias y la realización de una consulta pública, la PNCS fue lanzada oficialmente el 27 de abril del presente año (Subsecretaría de Defensa, 2017).

El presente informe tiene como objetivo medir el impacto de la participación de los distintos actores que fueron parte del proceso de elaboración de la Política. Para ello, se analizarán los comentarios presentados por dichos actores en el proceso de consulta pública del borrador de la PNCS. Del mismo modo, se analizarán las diferencias entre el borrador y la versión final de la PNCS, a fin de identificar modificaciones que puedan haber sido producto de alguna recomendación realizada por los participantes.

En la primera sección de este informe se describe sucintamente la PNCS, las motivaciones detrás de su producción, sus objetivos de política para el año 2022, las medidas de política pública diseñadas

1. El Mercurio, "Sigue creciendo el alcance del ciberataque: 270 detecciones en Chile y 75 mil a nivel mundial", 12 de mayo 2017, http://www.emol.com/noticias/Tecnologia/2017/05/12/858167/Sigue-creciendo-el-alcance-del-ciberataque-270-detecciones-en-Chile-y-75-mil-a-nivel-mundial.html (revisado el 10 de octubre de 2017)

para el período 2017-2018 y la institucionalidad propuesta para su implementación.

En la segunda sección se describe el proceso de participación en la elaboración de la PNCS y se analiza su nivel de inclusividad, transparencia y apertura. Para ello, se realiza una revisión bibliográfica de la literatura académica que trata el tema de la participación de múltiples partes interesadas en los procesos de elaboración de políticas públicas digitales. Del mismo modo, se describe el proceso de participación, tanto en la etapa de audiencias como de consulta pública, y se analiza su nivel de inclusividad, transparencia y apertura.

En la tercera sección se realiza una caracterización de los participantes en el proceso de consulta pública de la PNCS, dividiéndolos por categorías: sociedad civil, sector privado, instituciones públicas, academia, comunidad técnica o personas naturales. Luego, se analiza el contenido de los comentarios por categoría, a fin de discernir en qué temas los participantes pusieron énfasis al momento de proponer modificaciones.

La cuarta sección describe las principales modificaciones que sufrió el documento borrador al ser comparado con la versión final de la PNCS. Del mismo modo, se presentan a modo de ejemplo algunos comentarios de los participantes que coinciden con cambios realizados en la versión final del documento.

La quinta sección se avoca a describir las impresiones de los participantes en cuanto al nivel de apertura e inclusividad del proceso de participación de la PNCS, y hasta qué nivel estos participantes sintieron que sus comentarios y aportes fueron incorporados al documento final.

Por último, se presentan algunas conclusiones y recomendaciones relacionadas con la elaboración de la PNCS y cómo puede resultar ilustrativo para futuros procesos de elaboración de políticas públicas digitales.

2. METODOLOGÍA

El presente informe tiene como objetivo conocer el impacto qu tuvo la participación de los distintos actores en la elaboración de la PNCS. Para realizar dicho análisis es necesario abordar ciertos desafíos metodológicos.

El primer objeto de análisis son los participantes del proceso. Se realizó una caracterización de los mismos, que acaba en la existencia de seis categorías de participantes.[2]

Luego, surgen ciertas dificultades metodológicas al momento de optar por un método que pueda medir la incidencia de los aportes y sugerencias de los participantes en las modificaciones que sufrió el borrador de la PNCS y que derivó en su versión final. Cotejar el borrador de la PNCS, los comentarios de los participantes y la versión final no es suficiente para establecer un nexo causal entre el contenido del comentario y la consecuente modificación al borrador; incluso cuando la modificación parece tomada literalmente del comentario de alguno de los participantes, lo cierto es que para un espectador externo no hay forma de asegurar que la modificación se debió a dicho comentario y no a otro factor.

Tomando en cuenta este problema, optamos por dividir el análisis de la participación en el proceso de consulta pública en tres partes. En la primera se establece como objeto de análisis el contenido de los comentarios por categoría de los participantes. Esto permite desagregar los temas específicos que las distintas categorías de participantes decidieron priorizar en sus aportes.

En la segunda etapa del análisis se presentan de

2. Algunas prevenciones metodológicas debieron ser realizadas a fin de categorizar a ciertos participantes que se encontraban en zonas grises o cuyas actividades correspondían a múltiples categorías.

forma anecdótica casos en donde la modificación del borrador de la PNCS coincide fuertemente con el comentario de alguno de los participantes. Las modificaciones elegidas buscan representar al menos un caso por categoría.

Por último, para agregar un componente cualitativo al análisis, recogimos las impresiones de los participantes en cuanto a la apertura, transparencia e inclusividad del proceso, así como sus impresiones respecto de hasta qué punto sus aportes fueron incorporados. Estas impresiones fueron recogidas en una reunión celebrada el día 7 de julio de 2017 en las oficinas de Derechos Digitales, en donde fueron invitados un número representativo de participantes en el proceso de consulta pública de la PNCS.

3. LA POLÍTICA NACIONAL DE CIBERSEGURIDAD

3.1 El Comité Interministerial sobre Ciberseguridad

La necesidad de contar con una Política Nacional de Ciberseguridad fue recogida en el programa de gobierno de la presidenta Michelle Bachelet, el cual declara que "[hoy] resulta relevante que nos planteemos desarrollar una estrategia de seguridad digital que proteja a los usuarios privados y públicos contra posibles acciones de violación de fuentes de datos, junto con la protección de la privacidad de nuestros ciudadanos".[3]

A fin de cumplir con dicha promesa, el 27 de abril de 2015 fue creado el Comité Interministerial sobre Ciberseguridad (CICS) a través del Decreto Supremo N 533 de 2015. De acuerdo al artículo primero de dicho decreto, la misión de esta comisión asesora del Presidente de la República es proponer una política nacional de ciberseguridad y asesorar en la coordinación de acciones, planes y programas de los distintos actores institucionales en la materia.

Para el cumplimiento de esta tarea, el CICS contó con las siguientes funciones y atribuciones:

a) Asesorar al Presidente de la República en el análisis y definición de la política nacional de ciberseguridad, la que contendrá las medidas, planes y programas de acción específicos que se aplicarán para su ejecución y cumplimiento.
b) Identificar las amenazas actuales y potenciales en el ámbito del ciberespacio, proponiendo las acciones tendientes a superar las brechas que se identifiquen, y monitorear su cumplimiento.
c) Analizar y proponer las alternativas de estructura orgánica para la ciberseguridad en Chile.
d) Analizar y estudiar la legislación vigente aplicable en materia de ciberespacio, proponiendo las modificaciones constitucionales, legales y reglamentarias que sean necesarias.
e) Proponer al Supremo Gobierno formas de coordinación entre actores públicos y privados.

Para cumplir con su propósito, y de acuerdo al artículo tercero del decreto, el Comité está integrado por representantes permanentes e invitados de las siguientes instituciones:

- *Subsecretaría del Interior*
- *Subsecretaría de Defensa*
- *Subsecretaría de Relaciones Exteriores*
- *Subsecretaría General de la Presidencia*
- *Subsecretaría de Justicia*
- *Subsecretaría de Economía*
- *Subsecretaría de Telecomunicaciones*
- *Agencia Nacional de Inteligencia*
- *Subsecretaría de Hacienda, en calidad de invitado*

3. Michelle Bachelet "Programa de Gobierno Michelle Bachelet 2014-2018" (Chile, 2014) , página 57, http://www.subdere.gov.cl/sites/default/files/programamb_1.pdf (revisado el 10 de octubre de 2017)

4. Disponible en: https://www.leychile.cl/Navegar?idNorma=1079608&idParte= (revisado el 10 de octubre de 2017)

Los Ministerios de Seguridad y Defensa e Interior publicaron de forma conjunta, en marzo de 2015, un documento titulado "Bases para una Política Nacional de Ciberseguridad", cuyo objetivo era establecer la necesidad de contar con una PNCS, los ejes de la futura PNCS y un cronograma de trabajo.

3.2 Objetivos y contenido de la PNCS

La versión final del documento establece cuatro objetivos que justifican la elaboración de una Política Nacional de Ciberseguridad:

- *Resguardar la seguridad de las personas en el ciberespacio*
- *Proteger la seguridad del país*
- *Promover la colaboración y coordinación entre instituciones*
- *Gestionar los riesgos del ciberespacio*

Con el fin de materializar los objetivos señalados anteriormente, la PNCS divide su contenido en tres secciones: objetivos de política para el año 2022, funciones e institucionalidad, y medidas de política pública 2017-2018.

3.2.1 Objetivos de política para el año 2022

En esta sección se establecen los lineamientos generales que la Política Nacional de Ciberseguridad pretende alcanzar al año 2022, y los subobjetivos necesarios para concretarlos.

El primer objetivo consiste en contar con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos.

Para alcanzar dicho objetivo, la PNCS identifica como necesario: 1) establecer medidas técnicas para prevenir, gestionar y superar los riesgos cuando estos se verifican a fin de proteger la infraestructura de la información, 2) identificar y jerarquizar las infraestructuras críticas de la información, 3) contar con equipos de respuesta a incidentes de ciberseguridad, 4) implementar mecanismos estandarizados de reporte, gestión y recuperación de incidentes y 5) establecer estándares diferenciados en materia de ciberseguridad.

El segundo objetivo consiste en que el Estado vele por los derechos de las personas en el ciberespacio. Para lo anterior, resulta necesario 1) la prevención de ilícitos y generación confianza en el ciberespacio, 2) el establecimiento de prioridades en la implementación de medidas sancionatorias, 3) la existencia de prevención multisectorial, y 4) el respeto y la promoción de derechos fundamentales.

El tercer objetivo de la política para el año 2022 es que Chile desarrolle una cultura de la ciberseguridad en torno a la educación, las buenas prácticas y la responsabilidad en el manejo de tecnologías digitales a través de 1) la generación de una cultura de la ciberseguridad, 2) la sensibilización e información a la comunidad, y 3) la formación en materia de ciberseguridad.

El cuarto objetivo establece la necesidad de que Chile genere relaciones de cooperación en ciberseguridad con otros actores y participe activamente en foros y discusiones internacionales, a través de 1) la generación de una política internacional de en materia de ciberseguridad, 2) la cooperación y asistencia internacional, 3) reforzar la participación en instancias multilaterales de múltiples partes interesadas y 4) el fomento de normas internacionales que promuevan la confianza y seguridad en el ciberespacio.

Por último, el quinto objetivo establece que el país debe promover el desarrollo de una industria de la ciberseguridad, que sirva a sus intereses estratégicos, a través de 1) la innovación y desarrollo en materia de ciberseguridad, 2) el desarrollo del componente de ciberseguridad dentro del sector TIC, 3) la generación de estudios que caractericen

la industria e identifiquen dominios estratégicos, 4) contribuir a la generación de oferta por parte de la industria local, y 5) la generación de demanda por parte del sector público basado en los intereses estratégicos del Estado.

3.2.2 Funciones e institucionalidad

Como parte de su mandato, al CICS le correspondió proponer las alternativas de estructura orgánica para la ciberseguridad en Chile. Para ello, la PNCS señaló que la estructura organizacional en materia de ciberseguridad será materia de ley, y debe ser presentada por los actores institucionales responsables en la materia, sin señalar explícitamente cuáles serían estos. Del mismo modo, se propuso la creación de un consejo consultivo asesor, de integración multisectorial.

Mientras este proyecto de ley sobre ciberseguridad se tramita en el gobierno y el Congreso, la PNCS propone prorrogar de forma transitoria y ampliar el mandato del CICS, en cuanto a su función comunicacional, de coordinación y seguimiento de medidas presentadas en la PNCS. En materia de gestión de incidentes que se generen en la Red de Conectividad del Estado, se propone que dicha función sea asumida transitoriamente por el Equipo de Respuesta ante Incidencias de Seguridad (CSIRT) del Gobierno.

El hecho de que se haya pospuesto la definición del organismo que estará a cargo de la ciberseguridad y de qué ministerio depende puede responder a una forma de destrabar una falta de consenso al interior del proceso. Sin embargo, es importante recalcar que este elemento constituye una carencia en la PNCS, especialmente teniendo en consideración que las definiciones institucionales resultan clave al momento de establecer responsabilidades políticas claras al momento de la implementación, y que otros países de la región sí lo establecen en sus respectivas estrategias de ciberseguridad.

3.2.3 Medidas de política pública 2017-2018

En este apartado de la PNCS se establecen 41 medidas de política pública a "corto plazo", que deberán implementarse durante los años 2017 y 2018. Las medidas se encuentran presentadas usando una tabla, la que señala brevemente el contenido de la medida, las instituciones responsables de su implementación y el objetivo en el cual se enmarcan.

El hecho de que las medidas a corto plazo estén circunscritas a los años 2017 y 2018 coincide con el período de términos del actual gobierno. Sin embargo, no existe ningún tipo de priorización entre las medidas propuestas, ni un sistema de indicadores que permita hacer seguimiento a su cumplimiento. Por último, no se establece un mecanismo concreto de seguimiento, ni de análisis presupuestario, como sí se realizó en el proceso de Agenda Digital 2020.[5]

4. PROCESO DE PARTICIPACIÓN Y SU NIVEL DE INCLUSIVIDAD, TRANSPARENCIA Y APERTURA

4.1 Importancia de la participación multisectorial

Existe una creciente tendencia en la literatura especializada a resaltar la necesidad de que la elaboración de políticas públicas digitales sea realizada a través de procesos participativos y de múltiples partes interesadas.

Esto se debe, en parte, a la importancia de que las estrategias de ciberseguridad cuenten con un enfoque integral, que abarque aspectos económicos, sociales, educativos, jurídicos, técnicos, diplomá-

5. Disponible en: http://www.agendadigital.gob.cl/#/seguimiento/

ticos, militares y relacionados con inteligencia (OECD, 2012). En este sentido, la participación de los distintos actores interesados hace más probable que la elaboración e implementación de las políticas nacionales de ciberseguridad puedan armonizarse con el respeto a los derechos fundamentales, como la privacidad, la libertad de expresión y el debido proceso, así como los principios técnicos que han regido internet hasta la fecha, tales como la apertura, la universalidad y la interoperabilidad (Maciel, Foditisch, Belli y Castellón, 2016).

Se ha argumentado que, dado que la mayoría de la infraestructura de internet e encuentra en manos privadas o es administrado por organizaciones técnicas no estatales, la implementación de un modelo de múltiples partes interesadas no es solo una alternativa, sino una necesidad (Álvarez y Vera, 2016).[6]

4.2 Etapa de audiencias

A comienzo de 2015, luego de la publicación del documento titulado "Bases para una Política Nacional de Ciberseguridad",[7] el CICS realizó una serie de audiencias públicas, a las que se invitó a distintos actores a comentar el documento, así como a responder a distintas inquietudes del CICS y proponer temáticas no presentes en el documento. A dichas sesiones de audiencia pública asistieron, entre otros:[8]

- *Asociación Chilena de Empresas de Tecnología de Información*
- *Asociación Gremial de Desarrolladores de Software*
- *Cámara de Comercio de Santiago*
- *Carabineros de Chile*
- *Centro de Estudios en Derecho Informático*
- *CLCert (Grupo Chileno de Respuesta a Incidentes de Seguridad Computacional)*
- *Consejo de Rectores*
- *Defensoría Penal Pública*
- *DuocUC (Universidad)*
- *Fiscalía de Chile*
- *Fundación País Digital*
- *NIC Chile (Entidad encargada de la administración de nombres de dominio)*
- *Derechos Digitales*
- Poder Judicial
- Policía de Investigaciones
- Servicio de Impuestos Internos

4.3 Proceso de consulta pública

En base al documento titulado "Bases para una Política Nacional de Ciberseguridad" y las impresiones y recomendaciones recopiladas en la etapa de audiencias públicas, el CICS se avocó a la redacción del primer el borrador de la PNCS, que fue publicado en febrero de 2016.[9]

Este borrador fue sometido a consulta pública, de acuerdo a la Ley 20.500 sobre Asociaciones y Participación Ciudadana en la Gestión Pública, entre el 29 de febrero y el 18 de marzo de 2016. El ingreso de comentarios se realizó a través de un formulario en línea, en el que los participantes debían identificarse a sí mismos y la institución que representaban. El formulario contenía dos preguntas abiertas, una de carácter general respecto al documento y otra solicitando señalar errores de

6. Vale la pena mencionar que ambos autores fueron parte del Comité Interministerial de Ciberseguridad y participaron de la elaboración de la PNCS.

7. Disponible en: http://ciberseguridad.interior.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf (consultado el 10 de octubre de 2017)

8. Información disponible en: http://ciberseguridad.interior.gob.cl/participacion/ (consultado el 10 de octubre de 2017)

9. Documento disponible en: http://ciberseguridad.interior.gob.cl/media/2016/02/Borrador-Consulta-P%C3%BAblica-PNCS.pdf (consultado el 10 de octubre de 2017)

hecho o apreciación. Luego, se entregaba espacio para realizar comentarios a cada uno de los cinco ejes estratégicos, al esquema institucional y a las medidas de políticas públicas 2017-2018.
Una vez finalizado el proceso de consulta pública, los comentarios de los participantes se hicieron públicos en el sitio web del CICS.[10]

4.4 Nivel de apertura, transparencia e inclusividad del proceso

En una publicación anterior (Lara y Viollier, 2017) se ha advertido que los principales obstáculos para la participación de distintos actores en procesos colaborativos de elaboración de políticas públicas digitales en Chile son dos. Por una parte, el hecho de que muchas de las organizaciones no cuentan con recursos suficientes para participar de procesos de consulta pública. Por otra, el que muchas organizaciones sienten que no se justifica participar en dichos procesos, teniendo en cuenta que en el pasado sus propuestas no son debidamente consideradas o que los procesos no llegan a buen puerto.

En este sentido, resulta necesario rescatar varios elementos que muestran un genuino interés de parte del CICS por generar un proceso efectivamente participativo. Entre ellos, el hecho de que el primer borrador haya sido redactado tomando en consideración los elementos aportados por distintos participantes en el proceso de audiencias públicas, los esfuerzos del Comité para facilitar la participación de organizaciones ubicadas en regiones (no obstante la ausencia de audiencias en regiones), el hecho de que la consulta pública fuera abierta a todo tipo de participantes y que los comentarios fueron publicados de forma íntegra, señalando a qué organización corresponde cada uno. Entre los aspectos que pueden ser objeto de mejora, consideramos que la participación en el proceso fue entendida de forma bilateral entre el Comité y los participantes, sin que se generaran instancias formales de participación colectiva donde compartir y contrastar posiciones.

10. Disponibles en: http://ciberseguridad.interior.gob.cl/consulta-ciudadana/ (consultado el 10 de octubre de 2017)

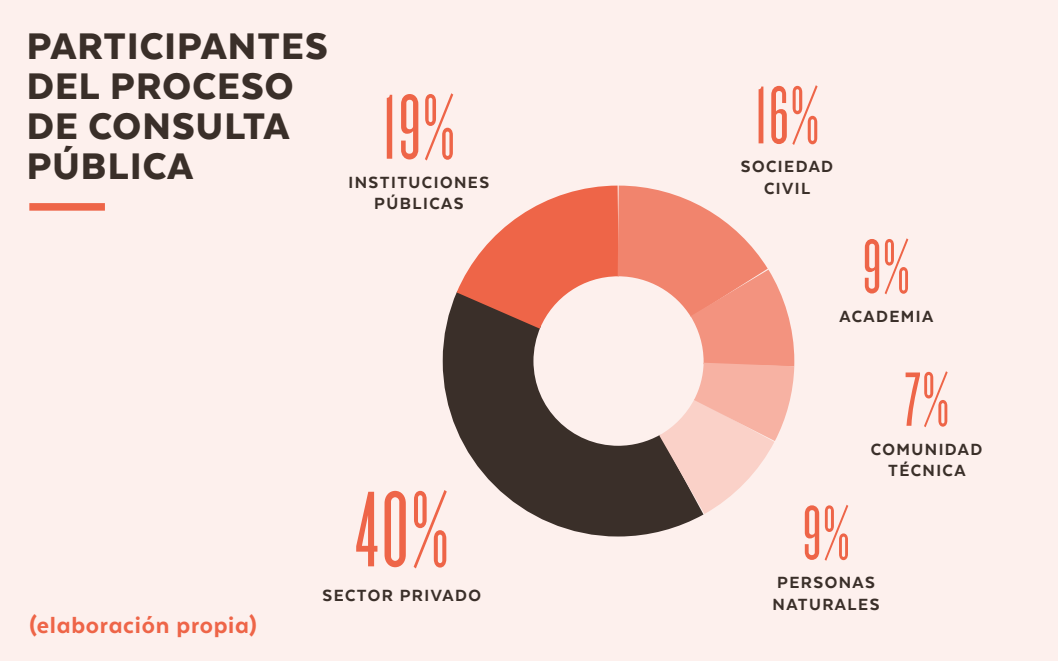
5. CARACTERIZACIÓN DE LOS PARTICIPANTES Y LOS COMENTARIOS EN EL PROCESO DE CONSULTA PÚBLICA

5.1 Los participantes

El proceso de consulta pública contó con la participación de 43 entidades, un número considerable en comparación con procesos anteriores de consulta pública en materia de políticas públicas digitales. Para efectos de este análisis, los participantes fueron divididos en seis categorías: sociedad civil, sector privado, instituciones públicas, academia, comunidad técnica y personas naturales.

Algunos de los participantes resultaron difíciles de clasificar, pues su naturaleza podía coincidir con distintas categorías. Es el caso de la Universidad de Chile, la cual es una institución académica que tiene la naturaleza jurídica de un organismo público, y en cuyo interior operan distintas entidades de la comunidad técnica. Finalmente, se decidió categorizarla como entidad académica y considerar como comunidad técnica a los organismos que operan a su alero, como NIC Chile y el CLCERT. Del mismo modo, a pesar de que la naturaleza jurídica de Fundación País Digital es la de una organización sin fines de lucro, fue colocada bajo la categoría de sector privado, por representar los intereses gremiales de la industria. Por último, cuatro personas presentaron comentarios a título personal sin arrogarse la representación de alguna organización. Estos cuatro participantes

TABLA 1: Porcentaje de participación por categoría de participante



(elaboración propia)

fueron dejados sin categoría, aun cuando parece probable que correspondan a algunas de las cinco categorías mencionadas.

De esta forma, de los 43 participantes, cuatro corresponden a la academia, tres a la comunidad técnica, 17 al sector privado, ocho a organismos públicos, siete a organizaciones de la sociedad civil y cuatro a personas naturales.

Como es posible apreciar, la participación de las empresas resultó predominante en el proceso de consulta pública. Esto puede explicarse, por un lado, por el carácter estratégico que significa la ciberseguridad para las empresas que dependen de la red para mantener su modelo de negocio y, por otro, por el hecho de que las empresas cuentan con mayores recursos humanos y económicos que les permitan sostener su participación en este tipo de instancias. Los organismos públicos también mantienen un nivel elevado de participación, lo cual también puede deberse a los recursos que tienen a su disposición y a sus intereses institucionales. La comunidad técnica, por su lado, fue la que presentó el menor porcentaje de participación. Esto se puede deber a la falta de recursos y de solidez institucional de sus organizaciones, así como también al hecho de que la PNCS era un documento de carácter legal y de política pública, lenguaje al que los miembros de la comunidad técnica pueden no encontrarse familiarizados.

5.2 Análisis de los comentarios por categoría

Como se mencionó antes, para un observador externo no resulta posible atribuir una conexión causal entre un comentario y una modificación específica del borrador de la PNCS. Por lo mismo, resulta necesario transformar los comentarios en el objeto mismo del análisis, a fin de entender las prioridades y énfasis que tuvieron los actores en la consulta pública, y así dilucidar cuales temas

TABLA 2: Cantidad de comentarios sustantivos por actor

ACTOR	Nº POR ACTOR	INFRAESTRUCTURA	PREVENCIÓN DE ILÍCITOS	PROTECCIÓN DE DERECHOS FUNDAMENTALES	EDUCACIÓN	COOPERACIÓN INTERNACIONAL	INDUSTRIA CIBERSEGURIDAD	INSTITUCIONALIDAD	TOTAL COMENTARIOS POR ACTOR
Academia	4	1	1	2	2	1	2	2	11
Comunidad técnica	3	3	2	3	3	1	2	3	17
Instituciones públicas	8	4	3	2	1	2	1	3	16
Sector privado	17	15	9	2	11	8	7	10	62
Sociedad civil	7	7	5	4	7	7	6	7	43
Personas naturales	4	0	1	1	1	1	0	2	6
Total comentarios por tema		30	21	14	25	20	18	27	155

(elaboración propia)

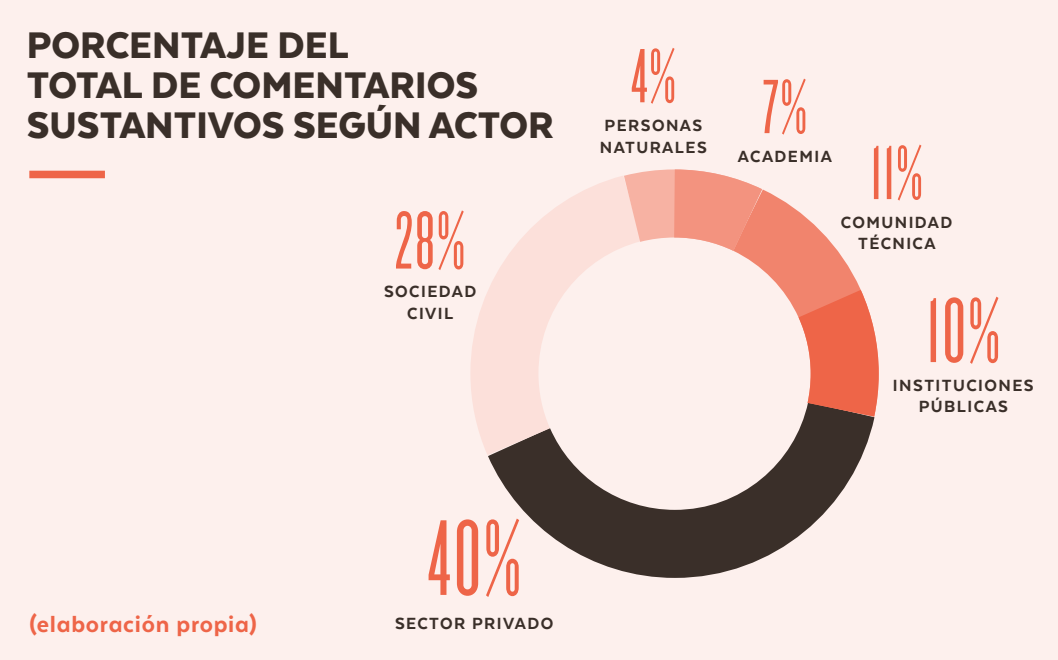
resultaron prioritarios al momento de intentar incidir en la versión final de la PNCS para cada categoría.

Para ello se analizaron los más de 400 comentarios ingresados por los 43 participantes en el proceso de consulta pública y los ejes temáticos en que se hicieron comentarios sustantivos o que dieran a entender un énfasis de interés en el tema.[11] Los ejes temáticos considerados son los mismos establecidos por la PNCS, los que por razones de simplicidad se denominarán: infraestructura, delitos informáticos, protección de derechos fundamentales, educación, cooperación internacional, industria de ciberseguridad e institucionalidad. Vale la pena mencionar que el eje B de la PNCS fue dividido en dos temas: delitos informáticos y protección de derechos fundamentales, ya que un gran porcentaje de los comentarios los trataban como temas separados.

Como es posible apreciar, el sector privado es quien más comentarios sustantivos aportó al proceso de consulta pública. Esto se puede deber a la cantidad de actores que pertenecen a esta categoría (40%). Por otro lado, la sociedad civil, siendo proporcionalmente menor su participación en términos de cantidad de instituciones participantes (16%) aportó una cantidad importante de comentarios sustantivos (43). Por el contrario, la academia solo aportó 11 comentarios sustantivos en total.

11. En este sentido, es importante hacer notar que solo se consideraron los comentarios que dieran a entender un genuino interés de la persona por desarrollar el tema. Aquellos comentarios simplemente formales o casuales serán considerados en blanco para el propósito de esta medición. Como se muestra en la Tabla 2, el total de comentarios considerados "sustantivos" equivale a 155.

TABLA 3: Porcentaje total de comentarios sustantivos por actor (elaboración propia)



Lo anterior puede observarse de forma más nítida al presentarse la cantidad de comentarios sustantivos por actor en términos de porcentaje. De esta forma, el sector privado mantiene una participación en términos porcentuales proporcional a la cantidad de participantes del proceso. Por otro lado, la cantidad de comentarios sustantivos de la sociedad civil es proporcionalmente mayor a su participación en términos de cantidad de instituciones participantes. Esto quiere decir que, en promedio, las organizaciones de la sociedad civil hicieron más comentarios sustantivos que el resto de los participantes. Algo similar, aunque en menor medida, sucede con la participación de la comunidad técnica.

Por otro lado, la academia y las instituciones públicas hicieron en promedio menos comentarios sustantivos en relación a su cantidad de participantes en el proceso.

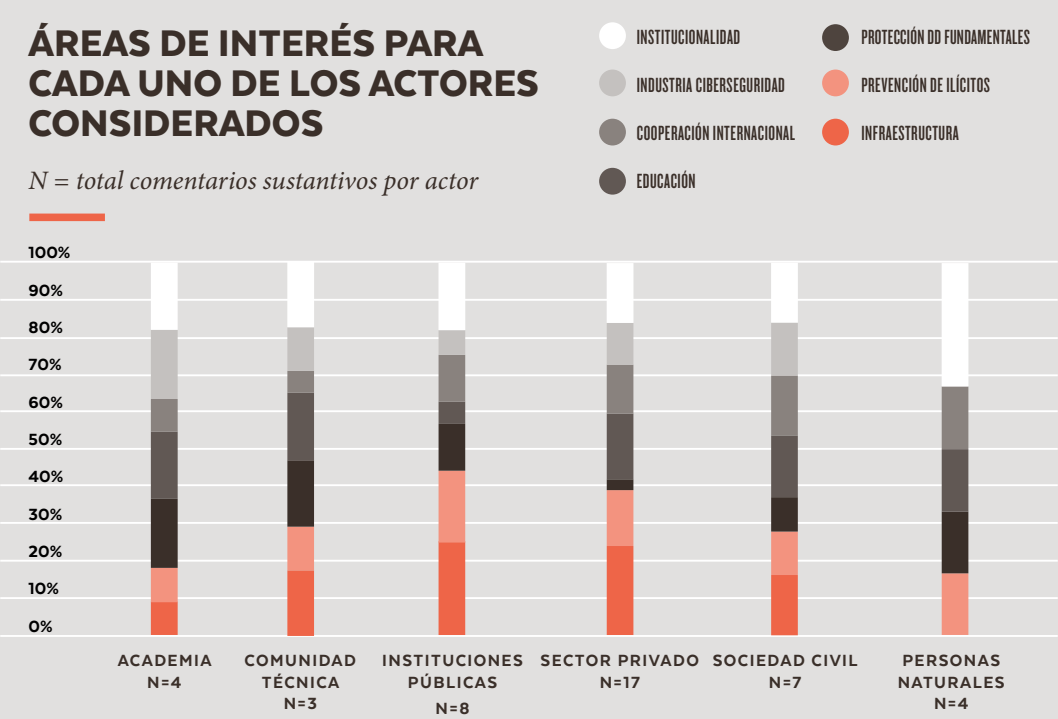
En base a los datos contenidos en la Tabla 2, es posible visualizar las áreas en que cada categoría de actor participó con más interés.

Entre los resultados, vale la pena dar cuenta que los comentarios de las instituciones públicas y el sector privado tuvieron un fuerte énfasis en el eje de infraestructura. Por otro lado, la academia, la comunidad técnica y las instituciones públicas fueron quienes más énfasis pusieron en el eje de derechos fundamentales.

Por su lado, llama la atención que la sociedad civil haya invertido más comentarios sustantivos en los ejes de infraestructura, educación, prevención del delito y cooperación internacional, que en el eje sobre derechos fundamentales.

Por último, resulta sumamente preocupante la falta de atención que mostró el sector privado en el eje de derechos fundamentales. Resulta necesario que un futuro proceso de investigación cualitativa ahonde en las eventuales causas de esta aparente falta de interés.

TABLA 4: Áreas de interés para cada uno de los actores involucrados



(elaboración propia)

6. DIFERENCIAS ENTRE EL BORRADOR Y LA VERSIÓN FINAL DE LA PNCS

En esta sección se detallan las partes que fueron agregadas a la versión final de la PNCS, qué partes fueron eliminadas del borrador y qué partes fueron replanteadas. Si bien el cotejo entre el borrador y la versión final de la PNCS muestra modificaciones sustantivas, resulta difícil atribuir un cambio particular a un comentario en específico.

Finalmente, se presentan aquellos comentarios que parecen coincidir con modificaciones particulares, lo que puede insinuar cierto nivel de impacto de la participación multisectorial en la versión final de la PNCS.

6.1 Principales incoporaciones

En cuanto al Objetivo A de la política para el año 2022, se agregó una definición del concepto de ciberseguridad y se estableció que la ampliación de la capacidad de vigilancia estatal o privada no forma parte del marco de ciberseguridad. Además se agregó una referencia a la necesidad de monitorear la seguridad de los sensores y dispositivos operados desde el ciberespacio. En lo relacionado con los equipos de respuesta a incidentes de ciberseguridad, la versión final se propuso promover la creación de CSIRT sectoriales por parte de distintos actores. Por último, se agregó una referencia a la necesidad de promover el reporte de vulnerabilidades informáticas por parte de usuarios y expertos,

evitando la recolección y procesamiento de datos que pueda afectar la privacidad de las personas.

La principal modificación al Objetivo B fue el cambio de título, de "El Estado velará por los derechos de las personas en el ciberespacio, mediante la prevención y sanción efectiva de delitos, garantizando el pleno respeto de los derechos humanos" a simplemente "El Estado velará por los derechos de las personas en el ciberespacio" en la versión final. Este cambio resulta positivo, pues el anterior daba a entender que la forma en que el Estado vela por los derechos de las personas en el ciberespacio (o al menos la más relevante) es a través de la sanción efectiva de los delitos, siendo esta solo una más de las diversas formas en que se protegen los derechos de las personas en el entorno digital.

Otro elemento relevante que se agrega a este objetivo es una referencia explícita al reconocimiento de las tecnologías de cifrado, estableciendo que las medidas basadas en esta política deberán promover el cifrado punto a punto. Del mismo modo, se señala que ninguna persona u organización deberá someterse a la obligación de implementar mecanismos de "puerta trasera". Sin embargo, ninguna referencia relativa a la eventual posibilidad de que el Estado incurra en actividades de *hacking*, ni su eventual marco de regulación fueron agregadas.

Por último, se agrega una referencia a que en materia de derechos fundamentales se considerarán especialmente los derechos de grupos vulnerables, además del empleo de un enfoque de género. Sin embargo, no se establecen parámetros claros respecto de lo que se entenderá por un enfoque de género, más allá de la inclusión del término.

El Objetivo C de la política no presenta adiciones sustantivas.

El Objetivo D de la política agregó una referencia a que la adhesión a la Convención de Ciberdelitos deberá realizarse efectuando las reservas y prevenciones consistentes con la PNCS.

El Objetivo E de política para el año 2022 no presenta adiciones sustantivas.

6.2 Párrafos modificados

Se replantea el primer acápite del Objetivo A de política para el año 2022 precisando la importancia de la creación de modelos de prevención y gestión de riesgos, a fin de prevenir, gestionar y superar los riesgos en el ciberespacio, cuando estos se verifiquen.

El Objetivo B de política para el año 2022 también sufrió una modificación, en particular en su apartado sobre respeto y promoción de derechos fundamentales. La redacción actual establece que todas las medidas propuestas por la política se deben diseñar y ejecutar con un enfoque de derechos fundamentales. Sobre lo anterior, resulta necesario destacar que no se establecieron criterios sobre qué deberá entenderse por un enfoque de derechos fundamentales y cuando dicho estándar se estaría incumpliendo. Esto debilita la capacidad de utilizar la PNCS como una herramienta para medir si una futura política pública es contradictoria con el enfoque de derechos fundamentales que se pretende establecer.

Por último, se replantea la gobernanza transitoria en ciberseguridad, prorrogando la existencia y ampliando el mandato del CICS respecto de su función comunicacional, de coordinación y seguimiento de medidas de la PNCS. Sin embargo, las funciones que se identifican como esenciales para la creación del nuevo servicio público encargado de la ciberseguridad son establecidas en términos menos precisos.

6.3 Comentarios incorporados

A continuación se presentan de forma ejemplar comentarios representativos de cada uno de las categorias de actores participantes que parecen haber sido incorporados de forma directa en la versión final de la PNCS:

Comunidad técnica:
(1) La definición del CSIRT Nacional debiera incluir entre sus objetivos el fomento a la creación de nuevos CSIRTs sectoriales […] y de apoyo/cooperación una vez en operación.
(2) La política debiera enunciar también medidas de fomento y apoyo normativo al reporte y notificación responsable de vulnerabilidades de software por parte de los ciudadanos a las organizaciones responsables de su desarrollo, vía mecanismos claros y públicos que incluyan el acompañamiento técnico del CSIRT Nacional […].[12]

Estos comentarios parecen haber sido recogidos por la versión final de la PNCS en el quinto párrafo del punto 4 del Objetivo A de la política (página 17) y en el párrafo quinto del punto 5 del mismo objetivo respectivamente (página 18). Sin embargo, a pesar de haber sido recogidos en los objetivos de la política al 2022, no fueron agregaron a las políticas a implementarse durante el período 2017-2018.

Sociedad civil:
(1) "Un objetivo razonable para la política al año 2022 debería ser velar por los derechos de las personas en el entorno digital, y dentro de ese objetivo, una de las medidas debería ser el velar por los derechos de las personas a través de un combate al cibercrimen. De la forma en que el objetivo está planteado, parece como si el prevenir y sancionar los delitos fuera la única forma que la PNCS concibe para velar por los derechos de las personas en el ciberespacio".[13]

Este comentario parece haber sido recogido en la modificación del título del Objetivo B de la política para el año 2022, comentada anteriormente.

Academia:
(1) "Yo agregaría el tema particular de criptografía y firma electrónica. Si logramos difundir su uso masivo, aportaremos un gran nivel de seguridad a todos nuestros datos y documentos".[14]

Este comentario parece haber sido incorporado en un párrafo nuevo del punto 1 del Objetivo B de la política para el año 2022, el que señala que se promoverá 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".[15]

Instituciones públicas:
(1) "Se recomienda comprometer el estudio de una nueva institucionalidad, sin ahondar respecto a su diseño, orgánico y de atribuciones, por cuanto es materia que debe definirse en el respectivo proyecto de ley".[16]

12. Comentario ingresado por el CLCERT, Universidad de Chile. Disponible en: http://ciberseguridad.interior.gob.cl/consulta-ciudadana/

13. Comentario ingresado por Derechos Digitales. Disponible en: http://ciberseguridad.interior.gob.cl/consulta-ciudadana/

14. Comentario ingresado por José M. Piquer Gardner a nombre de la Universidad de Chile. Disponible en: http://ciberseguridad.interior.gob.cl/consulta-ciudadana/

15. Política Nacional de Ciberseguridad, página 19.

16. Comentario ingresado por el Ministerio Secretaría General de la Presidencia. Disponible en: http://ciberseguridad.interior.gob.cl/consulta-ciudadana/

Este comentario parece haber sido recogido en el párrafo sobre institucionalidad para la ciberseguridad (página 25), el cual fue replanteado para establecer de forma menos específica las funciones que el nuevo servicio público propuesto a cargo de la ciberseguridad. No obstante, nada impide que el Comité proponga lineamientos más nítidos para los proyectos de ley correspondientes.

Sector privado:

(1) "Nos parece que debe agregarse que, debido a la naturaleza dinámica de la ciberseguridad, las iniciativas de evaluación de riesgos deben ser actualizadas regularmente como un proceso continuo".[17]

Este comentario parece haber sido incorporado a través de un párrafo nuevo en el objetivo A de la política para el año 2022, el que establece que *"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".*[18]

17. Comentario ingresado por Microsoft Chile S.A. Disponible en: http://ciberseguridad.interior.gob.cl/consulta-ciudadana/

18. Política Nacional de Ciberseguridad, página 16 (énfasis es nuestro).

19. Los participantes fueron invitados a la reunión en una proporción que resultara representativa de la participación que tuvieron en el proceso. Lamentablemente, ningún representante del sector privado pudo participar

7. IMPRESIONES DE LOS ACTORES SOBRE EL PROCESO DE PARTICIPACIÓN

A fin de agregar un elemento cualitativo al análisis de impacto de la participación multisectorial en el resultado de la Política Nacional de Ciberseguridad, se celebró una reunión de trabajo el día 7 de julio de 2017 en las oficinas de Derechos Digitales, con la finalidad de recabar la impresión del proceso de un número representativo de personas que participaron en él. A dicha reunión asistieron tres organizaciones de la sociedad civil (incluyendo a Derechos Digitales), dos organismos públicos (incluyendo a un representante del CICS), dos miembros de la comunidad técnica, un académico y ningún representante del sector privado.[19]

En cuanto al proceso de consulta pública, hubo consenso en cuanto a lo participativo del proceso, en particular comparado con procesos similares anterior. Se rescató que los comentarios fueran publicados de forma nominativa y, en general, la mayoría de los asistentes sintieron que, hasta cierto punto, algunos de sus comentarios fueron incorporados a la versión final de la PNCS. Muchos participantes mostraron preocupación de que ese mismo espíritu se mantuviera en la etapa de implementación, en particular por la falta de un organismo encargado del seguimiento de dichas medidas.

En este sentido, varios participantes señalaron que la forma en que se condujo el proceso de consulta pública en la PNCS debería transformarse en un nuevo piso mínimo en materia de participación. Sin embargo, miembros de la sociedad civil hicieron notar que todavía es necesario acercar estas materias a organismos menos especializados en temas de ciberseguridad, pero que pueden verse afectados, tales como organizaciones de usuarios y consumidores.

Por último, se dio una interesante discusión sobre la necesidad de permitir aportes realizados de forma privada y reservada, puesto que la publicidad puede impedir que ciertos actores interesados compartan información de carácter sensible.

8. CONCLUSIONES Y RECOMENDACIONES

El fenómeno de la ciberseguridad es de carácter complejo, multidisciplinario y multisectorial. Lo anterior justifica, y hasta cierto punto convierte en una necesidad, que los procesos de elaboración de políticas públicas en la materia se realicen a través de procesos de múltiples parte interesadas.

Esta modalidad permite incorporar distintas visiones y aproximaciones, así como recoger todos los antecedentes necesarios para que dichas políticas sean elaboradas en base a la evidencia. La participación multisectorial no solo vuelve los procesos más abiertos, transparentes y democráticos, sino que tiene el potencial de mejorar la calidad de los mismos, especialmente en temas sistémicos y que involucran diversos factores, como en la ciberseguridad.

En este sentido, el proceso de elaboración de la Política Nacional de Cibersegurdad de Chile se presenta como un caso de estudio positivo respecto a la influencia de la participación multisectorial en el resultado de las políticas públicas de ciberseguridad.

El análisis de los participantes y su naturaleza muestra que existe una predominancia de actores privados y de gobierno en la etapa de participación, lo que probablemente se explica por los mayores recursos que cuentan estas instituciones, además de posibles sesgos en la identificación de actores relevantes.

El estudio de los comentarios muestra que si bien participaron varios organismos públicos, lo hicieron en un número acotado de temas, probablemente relacionados con el ámbito de sus competencias. Del mismo modo, resulta preocupante la falta de participación en el eje de derechos fundamentales por parte de las empresas.

El cotejo de los comentarios entre el borrador y versión final de la PNCS da a entender que varios comentarios fueron incorporados de forma casi directa.

Las impresiones recolectadas entre los participantes del proceso son en general positivas, en especial en lo que respecta al nivel de apertura, transparencia y participación del proceso. Sin embargo, todavía persiste la preocupación de que el proceso de implementación pueda no resultar igual de positivo.

BIBLIOGRAFÍA

Álvarez, Daniel y Vera, Francisco. "*Ciberseguridad y derechos humanos en América Latina*", en Hacia una Internet libre de censura II: Perspectivas en América Latina; compilado por Agustina Del Campo . - 1a ed . - Ciudad Autónoma de Buenos Aires : Universidad de Palermo - UP, 2017.

Bachelet , Michelle. "*Programa de Gobierno Michelle Bachelet 2014-2018*" (Chile, 2014), http://www.subdere.gov.cl/sites/default/files/programamb_1.pdf (revisado el 10 de octubre de 2017)

El Mercurio, "*Sigue creciendo el alcance del ciberataque: 270 detecciones en Chile y 75 mil a nivel mundial*", 12 de mayo 2017, http://www.emol.com/noticias/Tecnologia/2017/05/12/858167/Sigue-creciendo-el-alcance-del-ciberataque-270-detecciones-en-Chile-y-75-mil-a-nivel-mundial.html (revisado el 10 de octubre de 2017)

Global Partners Digital. "*Framework for multistakeholder cyber policy development*", 7 de octubre 2017, https://www.gp-digital.org/publication/framework-for-multistakeholder-cyber-policy-development/ (revisado el 10 de octubre de 2017)

La Tercera, "*Casi 24 mil ciberdelitos se reportaron el primer semestre*", 16 de agosto 2017, http://www.latercera.com/noticia/casi-24-mil-ciberdelitos-se-reportaron-primer-semestre/ (revisado el 10 de octubre de 2017).

Lara, Juan Carlos y Viollier, Pablo. "*Mapping the Cyber Policy Landscape: Chile*", Global Partners Digital https://www.gp-digital.org/wp-content/uploads/2017/02/mappingthecyberlandscape_chile.pdf (revisado el 10 de octubre de 2017)

Maciel, Foditisch, Belli y Castellón. "*Seguridad cibernética, privacidad y confianza: tendencias en América Latina y el Caribe. El camino a seguir*", en Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, 2016. https://publications.iadb.org/handle/11319/7449

OECD. "*Cyberpolicy security policy making at a turning point: Analyzing a new generation of national cybersecurity strategies for the internet economy*". OCDE, 2012. P 12.

Piquer, José Miguel. "*Internet: Infraestructura Crítica*", 29 de septiembre de 2015, http://ingenieria.uchile.cl/noticias/115726/internet-infraestructura-critica (revisado el 10 de octubre de 2017)

Poder Judicial, "*Noticiero Judicial: Correo falso recibido por usuarios*", 29 de septiembre de 2014, https://www.youtube.com/watch?v=uWHkaeBZ-MM0 (revisado el 10 de octubre de 2017)

Subsecretaría de Defensa. "*Una Política Nacional de Ciberseguridad para Chile*", 27 de abril de 2017, http://www.ssdefensa.cl/n5427_27-04-2017.html (revisado el 10 de octubre de 2017)


DERECHOS
DIGITALES
América Latina