JULIO
2016

INFORME BREVE

VIGILANCIA EN CHILE: HACIA UNA POLÍTICA NACIONAL DE CIBERSEGURIDAD

PAULA JARAMILLO GAJARDO

@ | DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina

Este informe fue realizado como parte del trabajo Derechos Digitales en la Cyber Stewards Network, en el marco de un proyecto financiado por el International Development Research Centre, Ottawa, Canada.

Derechos Digitales:
Organización No Gubernamental fundada en el año 2005, 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 están la libertad de expresión, los derechos de autor y la privacidad.

Diseño y diagramación: Constanza Figueroa
Corrección: Vladimir Garay

Julio de 2016

INFORME BREVE

VIGILANCIA EN CHILE: HACIA UNA POLÍTICA NACIONAL DE CIBERSEGURIDAD

PAULA JARAMILLO GAJARDO

Introducción

En este documento de avance de investigación, examinaremos brevemente los contenidos más relevantes de la Propuesta de Política Nacional de Ciberseguridad (PNCS) 2016-2022,[1] preparada por el Comité Interministerial de Ciberseguridad al que hicimos referencia en el primer informe y que fue puesta a disposición para consulta pública por el Ministerio del Interior y Seguridad Pública de Chile a principios de 2016.

Sus planteamientos parten del análisis de los riesgos asociados al uso de las tecnologías de la información y comunicaciones, tanto en el contexto nacional como internacional, además del estado y las necesidades en materia de ciberseguridad que hacen preciso contar con una política nacional al respecto, con una mirada enfocada tanto en el presente como en el futuro.

Este documento considera el análisis de la propuesta dividida en dos partes principales: una relacionada con objetivos estratégicos para el año 2022 y otra sobre la agenda de medidas propuestas para el año en curso y el siguiente; además de un breve apartado referido a la institucionalidad y sus funciones. Asimismo, de acuerdo al eje de la presente investigación, expresamos las consideraciones que la propuesta merece en relación con la capacidad de vigilancia.

1 Disponible en: http://ciberseguridad.interior.gob.cl/media/2016/02/Borrador-Consulta-Pública-PNCS.pdf

Objetivos Estratégicos para el año 2022

La propuesta plantea cinco objetivos estratégicos a ser desarrollados conjuntamente por el Gobierno y el sector privado, relacionados con las áreas de infraestructura, derechos, cultura, relaciones de cooperación y promoción de la industria de la ciberseguridad.

El primero de ellos[2] está referido a la infraestructura de la información, con un particular énfasis en aquellas que resultan críticas para el país (infraestructura críticas de la información o ICI)[3], respecto de las cuales se propone no sólo la identificación, sino también su jerarquización.

Cabe mencionar que la finalidad genérica de este primer objetivo dice relación con la posibilidad de contar con la capacidad de respuesta suficiente ante incidentes de ciberseguridad. Para ello resulta clave el monitoreo previo, una gestión eficiente ante las dificultades y la posterior respuesta para que la infraestructura afectada pueda recuperarse y ser resiliente, esto es, aprender continuamente de los incidentes que se presenten a fin de adaptarse ante las dificultades futuras, manteniendo capacidad operativa.

Se contempla la exigencia de estándares diferenciados en materia de ciberseguridad, distinguiendo entre el nivel básico o mínimo y aquel aplicable a las ICI, debido a su sensibilidad, así como también la implementación de mecanismo de reporte, gestión y recu-

2 "A. El país contará con una infraestructura de la información pública y privada resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo un óptica de riesgos". Propuesta de Política Nacional de Ciberseguridad (PNCS) 2016-2022. Pág. 9.

3 La propia política define las ICI como aquellas "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." Op. Cit. Pág. 9.

peración de incidentes estandarizados, y la necesidad de contar con equipos de respuesta ante incidentes de seguridad, también llamados Computer Security Incident Response Team (CSIRT), tanto a nivel nacional como otros de carácter sectorial.

El segundo objetivo[4] se relaciona con los derechos de las personas en el ciberespacio, para lo cual se ha determinado como prioritario la prevención de ilícitos, incluso a nivel multisectorial, y la implementación de sanciones. Se pretende que lo anterior sea hecho respetando los derechos fundamentales, considerando que internet es un ambiente en el cual se aplican iguales derechos que en el mundo físico. Esto guarda una estrecha relación con la discusión sobre el uso de tecnologías intrusivas para la vigilancia dirigida en el contexto de la investigación criminal y de la recolección de información con fines de inteligencia.

Posteriormente, se aborda el desarrollo de una cultura de la ciberseguridad, fomentando la educación, sensibilizando e informado a la población, promoviendo las buenas prácticas y el manejo responsable de las tecnologías.[5]

Finalmente, esta propuesta también ha contemplado como objetivos el establecimiento de relaciones de cooperación y la participación a nivel internacional,[6] y la promoción de una industria de la ciberseguridad que sirva a los objetivos estratégicos del

4 "B. 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." Op. Cit. Pág. 11.

5 "C. Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales." Op. Cit. Pág. 13.

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

país, contribuyendo a su desarrollo digital.[7]

De forma seguida a la descripción de los objetivos, el documento se refiere sucintamente a las "Funciones e institucionalidad necesarias para desarrollar una política nacional de ciberseguridad", que contemplan la creación de un servicio público y un consejo consultivo asesor, sin demasiadas precisiones sobre su naturaleza, extendiéndose mayormente en el punto de las funciones requeridas,[8] para concluir señalando que dicha institucionalidad requiere de una implementación de tipo gradual.

En este apartado destaca que se haya omitido mencionar expresamente la participación de las organizaciones de la sociedad civil, la academia y la comunidad técnica en el contexto de la formación del señalado "consejo consultivo asesor, de integración público-privada", tal como reza el documento, persistiendo la duda si dicha denominación sólo abarcará al Estado y a las empresas.

Agenda de Medidas propuestas para el período 2016-2017

Se trata de un extenso y detallado listado de 42 medidas,[9] a ser desarrollado durante el presente año y el venidero, cada una de las cuales está vinculada con uno o más de los objetivos planteados para el año 2022 preliminarmente en el mismo documento de la propuesta.

Contiene un catálogo de medidas relacionadas con ciberseguri-

7 "E. El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos." Op. Cit. Pág. 15.

8 Se identifican las siguientes funciones: gestión de incidentes y de relaciones interinstitucionales, normativa general y normativa técnica, de seguimiento y evaluación de la implementación de las medidas propuestas, y de comunicaciones. Op. Cit. Pág. 17.

9 El listado completo está disponible en el documento "Propuesta de Política Nacional de Ciberseguridad (PNCS) 2016-2022". Pág. 19 a 22.

dad de menor complejidad y bastantes específicas, tales como la "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." (Nº 4), "identificar un set mínimo de riesgos para las infraestructuras criticas de la información." (Nº 8), o "instaurar el mes de la Ciberseguridad en octubre de cada año, promoviendo actividades de sensibilización en todos los niveles." (Nº 17), que se entremezclan con otras que apuntan a materias bastante más laboriosas tales como la generación o actualización de normativa ("1. Enviar al Congreso Nacional un proyecto de Ley sobre ciberseguridad, para consolidar institucionalidad y manejo de incidentes de seguridad informática en el país.", "2. Actualizar el DS 83 sobre seguridad de la información del Estado.", "3. Actualizar normativa sobre delitos informáticos."), cuyo desarrollo claramente será de mayor aliento que el bienio señalado.

Además, dicho listado de medidas no parece responder a una lógica de jerarquización, gradualidad o desarrollo en el tiempo, ya que no se han agrupado de una forma tal que faciliten su comprensión y seguimiento atendido el ámbito al que afectan. En términos amplios, apuntan al estudio y actualización de normativas, y a la propuesta de aquellas faltantes, a la conformación de grupos de expertos para el trabajo de temas específicos, la generación de estudios y la elaboración de documentos relativos a la materia.

Por otra parte, se trata de un plan ambicioso, ya que de las 42 medidas propuestas, 33 - equivalentes a un 78,57 %- se han programado para ser ejecutadas durante el año en curso (2016), en tanto solo las restantes nueve (21,42 %) están contempladas para el año 2017.

Propuesta de Política Nacional de Ciberseguridad y Vigilancia

En términos generales, la Propuesta de Política Nacional de Ciberseguridad levanta la preocupación por la adopción de medidas de investigación criminal y de recolección de información con fines de inteligencia, allí donde ello pueda significar amenazas a los

derechos fundamentales, incluidas la privacidad y el debido proceso. En tal sentido, dentro del objetivo de que el Estado vele por "los derechos de las personas en el ciberespacio", la propuesta expresa:

Para un equilibrio entre los beneficios que ofrece el ciberespacio y la seguridad que requiere, todas las medidas propuestas por la política se deben diseñar y ejecutar con pleno respeto a los derechos fundamentales, atendido su carácter universal e indivisible y sobre la base que el ciberespacio es un ambiente donde las personas cuentan con los mismos derechos que en el mundo físico. Así, la política considera y promueve:

> (…) La protección de la vida privada y el debido proceso, 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.

De entre las medidas relevantes para fines del presente estudio, destacan las medidas Nº 25 ("revisar las normas internacionales en materia de ciberespacio, con especial énfasis en instrumentos de derecho internacional y su aplicación"), Nº 39 ("adherir e implementar la Convención sobre Ciberdelitos del Consejo de Europa", o Convención de Budapest), junto a otras referidas al contexto internacional.[10] Junto a ellas podemos mencionar una nueva regulación sobre ciberdelitos para Chile, en la medida Nº 13 ("actualizar normativa sobre delitos informáticos").

Ahora bien, tanto la renovación legal interna propuesta como la adopción de la Convención de Budapest pueden significar una reescritura de las reglas bajo las cuales se entiende que la intrusión sobre un equipo constituye un acto delictual, con efectos que el

10 En esta situación se encuentra, por ejemplo, lo señalado en la medida propuesta Nº 27: "propiciar el intercambio de experiencias con otros países en materia de ciberseguridad, con énfasis en la implementación y evaluación de estrategias y políticas."

propio documento no permite predecir adecuadamente.

Especialmente relevante en este contexto es la propuesta Nº 15 ("promover el fortalecimiento de las capacidades de investigación y análisis forense relacionadas con el ciberdelito"), en atención a que tales capacidades de investigación podrían ser potenciadas con el uso de recolección de información mediante vigilancia de comunicaciones. Cabe mencionar que, bajo el actual esquema de penalización de ciberdelitos en Chile, la penalidad por los delitos contenidos en la ley Nº 19.223, sobre delitos informáticos, no es lo suficientemente alta como para hacer procedentes las medidas de vigilancia de comunicaciones permitidas por el artículo 222 del Código Procesal Penal, referido a la interceptación de comunicaciones, y es dudoso que puedan extenderse medidas similares con base a la ley Nº 19.974 que se refiere a los servicios de inteligencia y su operación para la seguridad nacional.

Mención aparte merece la inclusión en el documento de la vigilancia como un riesgo del ciberespacio. Dentro del panorama de riesgos que esboza la propuesta en su cuerpo principal, como también en sus anexos, se incluye a las actividades de espionaje y vigilancia llevadas a cabo por actores estatales. Para la propuesta, tales actividades afectan "la confidencialidad, integridad y disponibilidad de los activos de información en el ciberespacio, y con ello, los derechos de las personas". Sin embargo, al mismo tiempo que destaca esta apreciación, brilla por su ausencia una expresión afín de preocupación por las actividades de vigilancia y espionaje que pudieran ser llevadas a cabo por organismos del propio Estado chileno.

Conclusiones

En términos generales, en la política propuesta se aprecia la existencia de un trabajo de diagnóstico previo de la situación actual en materia de ciberseguridad en Chile, considerando las normas e instituciones actualmente existentes e identificando los riesgos presentes.

Sin embargo, de la medidas agendadas emana claramente que aún existe análisis pendiente, por ejemplo cuando se contempla la necesidad de "revisar las normas internacionales en materia de ciberespacio, con especial énfasis en instrumentos de derecho internacional y su aplicación" (Nº 28), además de la realización de estudios (medidas Nº 30 y 31).

Particularmente interesante resulta ser el que se haya identificado a nuestro país como uno de los principales blancos de ciberataques recientes,11 así como también la detección de una disminución en la comisión de ciberdelitos, a pesar de que su complejidad se ha acentuado, lo que da cuenta de la importancia del tema que la política aborda.

Sin duda la propuesta es una buena herramienta en tanto hoja de ruta, que detecta y ordena los elementos actualmente existentes y evidencia aquellos que es preciso incorporar, aún cuando denota un interés por suplir falencias que no son propias de ciberseguridad, sino de una adecuada política digital, mezclando aspectos eminentemente técnicos con otros relacionados con el contenido e incluso que derechamente competen a otras áreas. Así sucede, por ejemplo, con la medida que pretende "tramitar nueva ley de datos personales, con facultades a un órgano especifico que pueda imponer requisitos de seguridad y de notificación de filtraciones de datos" (Nº 32).

11 Op. Cit. Pág. 28.

De concretarse, todo este proceso requerirá de especial cuidado, ya que se trata de una propuesta no exenta de ambición, en el sentido de que contempla un abultado número de medidas a ser ejecutadas en breve plazo -durante el año que ya ha comenzado (2016) y sin que aún se haya aprobado el documento que fijará el punto de partida- con escasos indicadores que permitan medir el cumplimiento de las metas trazadas, pudiendo terminar en una mera declaración de buena intenciones.

En efecto, cabe recordar que la propia propuesta repite insistentemente el concepto de promover la confianza en el ciberespacio, e incrementar su seguridad, nada de lo cual podrá se logrará si se retarda indefinidamente el cumplimiento de las metas propuestas. En este sentido, es valorable que se hayan contemplados años determinados para la ejecución de las 42 medidas que el documento propone, sin embargo persiste el temor de que se trate de plazos poco realistas que terminen por hacer fracasar las medidas incluso antes de empezar a implementarse.

También en materia de plazos es preciso señalar que la propuesta confunde conceptos, al señalar que sus distintas medidas abarcan tanto el corto, como el mediano y largo plazo. En la realidad la agenda solo se refiere a medidas y a objetivos de corto y mediano plazo (6 años máximo), nada en ella se proyecta específicamente al largo plazo, usualmente entendido como el de 10 años o más, de no ser por los productos que de esta política puedan emanar y que perduren en el tiempo, como la promulgación de una ley relativa a ciberseguridad. Lo anterior resulta entendible desde una perspectiva política, pero llama a confusión en el lector.

Finalmente, señalar que se trata de una propuesta omnicomprensiva, considerando su enfoque desde el diagnóstico y apuntando hacia las medidas que es necesario adoptar para introducir de lleno el tema de la ciberseguridad, no solo en el quehacer del Estado, sino también en el de los privados, conformando una

estrategia de abordaje conjunto y desde múltiples ámbitos.

Sin embargo carece de la profundidad necesaria para llevar a cabo las medidas que se propone en el corto plazo, introduciendo una serie de conceptos que no define ("cultura de la ciberseguridad", "incidentes de ciberseguridad", por mencionar algunos); y en otros casos, lanzando ideas que a primera vista parecen muy necesarias e importantes, pero que, luego de un segundo análisis, resultan ser demasiados generales (adhesión a la convención de Budapest sin señalar el necesario análisis previo y reservas del caso; velar por los derechos de las personas mediante la implementación de medidas sancionatorias con respeto a los derechos fundamentales, sin que nada se diga acerca de otras formas de velar por los mismos derechos, ni acerca de las medidas de vigilancia llevadas a cabo por el propio Estado respecto de sus ciudadanos, entre otras), lo que termina por hacer surgir aún más dudas respecto a cómo serán desarrolladas posteriormente y en detalle, siempre que encuentre la viabilidad política necesaria para ello.

Bibliografía Consultada

Propuesta de Política Nacional de Ciberseguridad (PCNS) 2016-2022. En: http://ciberseguridad.interior.gob.cl/media/2016/02/Borrador-Consulta-Pública-PNCS.pdf


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina