Ministerio del Interior y Seguridad Pública

Ministerio de Defensa Nacional

BASES PARA UNA

POLÍTICA NACIONAL DE CIBERSEGURIDAD*

MARZO DE 2015

*Documento de trabajo elaborado por la Subsecretaría del Interior del Ministerio del Interior y Seguridad Pública y la Subsecretaría de Defensa Nacional del Ministerio de Defensa Nacional.

Contenido

1. Resumen

El presente documento orienta las bases para el diseño de una política nacional de ciberseguridad («PNCS»), a fin de preparar la adopción de decisiones de política pública en esta materia.

El desarrollo y la masificación en el uso de las tecnologías de información y comunicaciones, conlleva una serie de riesgos que afectan los derechos de las personas, las infraestructuras críticas de la información y los intereses vitales de Chile, a nivel nacional e internacional.

Estos riesgos pueden provenir de múltiples fuentes y resultar en fenómenos cuyas consecuencias pueden afectar de manera grave a la seguridad pública, los derechos fundamentales, e inclusive comprometer la seguridad externa del país mediante actividades de espionaje y ciberataques llevados a cabo por otros países, grupos organizados, o, incluso, por sujetos individuales.

A nivel internacional, existe un importante desarrollo en la materia. Al año 2013, más de 35 países contaban con algún tipo de estrategia o política de ciberseguridad y países como Holanda y Estonia ya llevan más de una versión. Ello ha facilitado que la comunidad internacional presente una considerable evolución doctrinaria, técnica y normativa en diversos foros, como Naciones Unidas, OEA, Unión Europea, entre otros, tanto desde una perspectiva de seguridad internacional como de seguridad interna en cada país.

A nivel nacional, el desafío es diseñar, implementar y poner en marcha las medidas que sean necesarias para proteger la seguridad de los usuarios del ciberespacio. Atendiendo a esta situación y considerando las necesidades nacionales, el programa de Gobierno de la Presidenta Michelle Bachelet contempla **"desarrollar una estrategia de seguridad digital que proteja a los usuarios privados y públicos".**

En este sentido, una política de ciberseguridad para Chile es necesaria para: i) resguardar la seguridad de las personas en el ciberespacio; ii) proteger la seguridad del país; iii) promover la colaboración y coordinación entre instituciones; iv) gestionar los riesgos del ciberespacio.

Una PNCS entrega orientaciones y líneas de acción de aplicación general para la implementación y evaluación de diversas actividades tendientes a minimizar estos riesgos y amenazas del ciberespacio en el país, las cuales se deberán implementar tanto respecto del sector público como del privado.

De acuerdo a lo anterior, se propone desarrollar cinco líneas de trabajo, que a su vez agrupan y sistematizan una serie de materias y medidas para ser diseñadas e implementadas en el corto, mediano y largo plazo, mediante el establecimiento de un grupo de trabajo interministerial. El documento concluye proponiendo un plan de trabajo que permita la formulación y ejecución de una política de ciberseguridad en el Estado de Chile.

2. Objetivo del documento

El presente documento señala las bases para la construcción de una política nacional de ciberseguridad («PNCS»), a fin de preparar la adopción de las políticas públicas que protejan la seguridad del país, sus instituciones y los derechos de las personas en este ámbito.

Para efectos de este texto, el **ciberespacio** será entendido como un ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior. Al hablar de **ciberseguridad**, nos referimos a una condición caracterizada por un mínimo de riesgos y amenazas en el ciberespacio, y especialmente al conjunto de políticas y técnicas destinadas a lograr dicha condición.[2]

3. Diagnóstico

3.1. Aproximación al problema

El concepto de ciberespacio data de la década de 1980, con el desarrollo de las tecnologías de la información y las telecomunicaciones. Dentro de este ambiente se multiplican las relaciones e interacciones sociales para la comunicación, intercambio de datos o desarrollo de negocios. Enmarcado dentro de esa tendencia, muchas infraestructuras críticas de los países (electricidad, agua, banca, transportes) ocupan el ciberespacio en sus procesos.

Lo anterior puede constatarse en el informe de la Unión Internacional de Telecomunicaciones (UIT), denominado "Medición de la Sociedad de la Información 2014", el cual estima que: "a finales de 2014, casi 3000 millones de personas estarán utilizando Internet, en comparación con 2.700 a finales de 2013", lo que supone un crecimiento de 300 millones de usuarios en el último año a nivel mundial. En tanto, el mismo organismo estimaba al año 2014 que un 66,5% de los chilenos utilizaban Internet.

Este desarrollo conlleva riesgos asociados al uso del ciberespacio que afectan los derechos de las personas, las infraestructuras críticas de la información y los intereses vitales de Chile a nivel nacional e internacional. Los riesgos pueden provenir de múltiples fuentes y resultar en fenómenos cuyas consecuencias pueden afectar de manera grave la seguridad pública, e inclusive comprometer la seguridad externa del país mediante actividades de espionaje y ciberataques llevados a cabo por otros países, grupos organizados o personas.

En este sentido, podemos entender la ciberseguridad como un fenómeno sistémico, multisectorial y transnacional. Sistémico, porque configura un sistema determinado por su componente más débil. Multisectorial, porque involucra a diversos actores, trascendiendo el ámbito del sector público y transnacional porque excede el ámbito de las fronteras nacionales, siendo transfronteriza y potencialmente global.

A nivel internacional, existe un considerable desarrollo en la materia. Diversos organismos internacionales como Naciones Unidas, vienen trabajando el tema desde hace más de quince años. Por ejemplo, desde 1998 la Asamblea General ha convocado periódicamente a un grupo de expertos

[2] Ver glosario al final de este documento

que analizan las amenazas provenientes del ciberespacio y proponen medidas de comportamiento responsable en el mismo.

Según datos de *European Network and Information Security Agency*[3] (ENISA), al año 2013 más de 35 países contaban con una Estrategia Nacional de Ciberseguridad (ENCS) y países como Holanda y Estonia ya llevan más de una versión. Otros países como por ejemplo el Reino Unido, cada año realiza un proceso de evaluación de esta estrategia, lo que ayuda al desarrollo y perfeccionamiento de la misma.[4] Esto ha posibilitado que la comunidad internacional especializada presente importantes avances técnicos, doctrinarios y normativos, en los distintos foros existentes, tanto desde una perspectiva de seguridad internacional como seguridad interna de cada país.

La naturaleza masiva del fenómeno, implica que la toma de decisiones en estas materias contemple procesos de participación donde, además del Estado, sea involucrado el sector privado y la sociedad civil. A nivel global, la mayoría de los foros internacionales sobre ciberseguridad consideran el principio de participación de múltiples sectores.[5]

En Chile, no existe a la fecha una política pública que se haya hecho cargo de este fenómeno, siendo necesario asumir el desafío de proponer acciones que permitan enfrentar las vulnerabilidades, riesgos y amenazas que genera la interacción en el ciberespacio, tanto para el país como para la comunidad internacional.

3.2. Descripción de las amenazas

En atención a la naturaleza global del ciberespacio, las fuentes de las amenazas provienen tanto de Chile como del exterior, y se originan tanto en actividades delictuales conducidas desde el país o a través de terceros países, como en actividades de espionaje y vigilancia llevadas a cabo con diversos fines, las que afectan la confidencialidad, integridad y disponibilidad de los activos de información en el ciberespacio.

A nivel global, existen abundantes antecedentes sobre ciberataques consistentes en actividades de espionaje y ataques de denegación distribuida de servicio (DDoS)[6] 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.

---

[3] National Cyber Security Strategies in the World, ENISA, disponible en http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[4] Disponible en http://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/

[5] Un proceso de participación conocido como "Multistakeholderism", principio por el cual se rigen espacios como las conferencias del ciberespacio y el Foro de Gobernanza de Internet.

[6] Sigla en inglés para "ataque distribuido de denegación de servicio", un tipo de ataque efectuado desde múltiples computadores para saturar las capacidades de conexión y/o procesamiento de un servidor conectado a Internet.

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

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 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%).[7]

En Chile, la Red de Conectividad del Estado (RCE) ha sufrido numerosos ciberataques. Por ejemplo, hay registro de incidentes por agresiones de DDoS o hackeos a sitios webs gubernamentales, observándose un importante crecimiento de éstos entre el 2010 y 2013. Asimismo, durante el año 2014, en la red gubernamental se detectó la siguiente muestra de patrones maliciosos:

Cuadro Nº1: Cantidad de patrones potencialmente maliciosos detectados en la Red de Conectividad del Estado (RCE) durante el periodo 2014

Regla de detección de patrón potencialmente malicioso	Cantidad de Registros	Descripción	Riesgo
ET TROJAN IRC Nick change on non-standard port	15.604.034	Utilización de puertos no estándares para comunicaciones del tipo IRC (posibles botnet)	Equipos potencialmente infectados, con riesgo de participación en botnet. Expone al usuario/institución a acciones judiciales por parte de terceros.
SPAM Outbound	11.411.276	Posible emisión de mail categorizable como spam o correo basura.	Posibles equipos enviando spam con riesgo a imagen institucional y posible fuga de información.
GPL SNMP public access udp	8.528.926	Intentos de acceso a dispositivos utilizando el protocolo de gestión de red SNMP	Posible acceso a información operacional de los equipos de comunicaciones que soportan la red institucional, exponiendo información sensible que puede ser utilizada para ataques posteriores a la infraestructura.
ET SCAN Potential SSH Scan	6.936.649	Intentos de detectar apertura de puertos de administración cifrados en dispositivos servidores y/o de comunicaciones	Posible acceso a puertos de administración de equipos de comunicaciones que en una segunda fase de este patrón malicioso pueden optar a un ataque de fuerza bruta y obtener control del equipo afectando la disponibilidad del servicio o bien poniendo en riesgo la información de la red.
BLACKLIST DNS	4.046.747	Requerimientos DNS	Equipos potencialmente infectados con riesgo

[7] 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.

request for known malware domain msnsolution.nicaze .net - Genome Trojan		por dominios reconocidos como malware.	de participación en botnet y/o compromiso de la información del equipo.
GPL DNS named version attempt	3.588.402	Intentos de obtener información de los DNS (Servidores de Nombre)	Posible acceso a información operacional de los servidores de nombre de la red que soportan la internet institucional. Esta información sirve para armar ataques más complejos sobre estos sistemas y afectar a los servicios.
GPL WEB_SERVER 403 Forbidden	2.789.426	Accesos a URL restringidas en los sitios web	Búsqueda de potencial acceso a información restringida en los portales web.
SERVER-WEBAPP WordPress XMLRPC potential port-scan attempt	2.693.339	Posibles escaneos a gestor de contenidos Wordpress	Un tipo de ataque a aplicaciones web para lograr afectar el servicio mismo y/o la información que este gestiona.
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2.262.405	Posibles ataques de amplificación DNS	Tráfico generado maliciosamente para afectar a terceros usando nuestros DNS, dañando la imagen institucional y afectando el ancho de banda de la red.
ET TROJAN MS Terminal Server User A Login, possible Morto inbound	1.857.567	Intentos de conexión a equipos de manera remota.	Posible acceso remoto al control de equipos, comprometiendo la información del mismo.
ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port Opcode 6 or 7 set	1.796.026	Tráfico no DNS fluyendo a través de los puertos estándares de DNS.	Potencial violación de políticas de privacidad corporativa al estar fluyendo información por canales destinados a otras funciones.
ET SCAN Cisco Torch SNMP Scan	1.744.467	Intentos de escaneo a los puertos de gestión de redes utilizando la herramienta Cisco-torch	Posible acceso a información operacional de los equipos de comunicaciones que soportan la red institucional, exponiendo eventualmente información sensible que puede ser utilizada para ataques posteriores a la infraestructura.
ET SCAN Potential VNC Scan 5900-5920	1.331.303	Potencial escaneo en busca de puertos de control remoto.	Posible acceso remoto al control de equipos, comprometiendo la información del mismo mediante equipos (servidores) que pudieran tener implementada la aplicación VNC.

Fuente: División Informática del Ministerio del Interior, año 2015

De acuerdo con el Ministerio Público, en relación con el cibercrimen, entre los años 2009 y 2013, el número de casos ingresados bajo el rótulo "delito informático" fue de 3.063 casos, distribuidos como se indica a continuación:

Cuadro N°2: Casos ingresados por ciberdelitos 2009 – 2013 por Ministerio Público

Año Casos ingresados	2009	2010	2011	2012	2013	Total
Total de ambos delitos	366	582	767	724	624	**3063**

Fuente: ULDDECO, Ministerio Público, 2014.

Por su parte, según los datos aportados por la Policía de Investigaciones (PDI), durante el periodo 2009 - 2013, se realizaron un total de 1.980 investigaciones, distribuidos como se indica a continuación:

Cuadro N°3: Investigaciones efectuadas por ciberdelitos 2009 – 2013 por PDI

Año Investigaciones efectuadas	2009	2010	2011	2012	2013	Total
Delito Informático	322	485	466	378	329	**1980**

Fuente: Brigada de Cibercrimen, PDI, 2014.

De esta forma, se puede constatar que los delitos informáticos tuvieron un ascenso hasta el año 2010, y luego un decrecimiento. En este sentido, la PDI explica el comportamiento debido a que la orientación del fenómeno mutó. En efecto, ocurrieron delitos informáticos en menor cantidad, pero más complejos en su ejecución, generando la necesidad de más recurso humano, así como también, de tecnología para dar adecuado tratamiento a estos nuevos delitos. 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.

Todo lo anterior constituye una amenaza para la seguridad, privacidad y confidencialidad en Internet, y afecta a todos sus usuarios, impidiéndole ejercer sus funciones, 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.

Es imprescindible hoy en día contar con estrategias de gestión y minimización de riesgos que consideren esta clase de amenazas, especialmente en lo referente a la infraestructura crítica 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.

4. Necesidad de una Política Nacional de Ciberseguridad

Producto de la facilidad de acceso a internet y a equipos informáticos, el ciberespacio es una fuente cada vez más considerable de riesgos y amenazas, situación de la que Chile no está exento. Los delincuentes y espías buscan naciones con bajos estándares de seguridad en el ciberespacio, para instalar redes y bases de operaciones para sus organizaciones, que pueden ser físicas o virtuales. Esto no sólo daña la imagen del país sino que puede tener efectos sociales y económicos. Al respecto, Chile debe ser un actor proactivo frente a la materia.

Una política en este ámbito también debe tener como uno de sus puntos de partida el respeto a los valores democráticos y a la Constitución Política de la República, especialmente en lo respectivo al respeto y promoción de los derechos y garantías fundamentales contempladas tanto en ese cuerpo como en acuerdos internacionales de derechos humanos.

Desde ese punto de vista, la PNCS se concibe desde una perspectiva de maximización y armonización de las garantías fundamentales de las personas, como el debido proceso, la libertad de expresión, el acceso a la información y a la protección de la vida privada, entre otras. Dado que el ciberespacio es un ambiente donde las personas cuentan con los mismos derechos que en el mundo físico, una política de ciberseguridad no incidirá negativamente en el goce o ejercicio de éstos[8].

Merecen una consideración especial los derechos fundamentales de igualdad ante la ley y no discriminación, toda vez que una política de estas características debe ser inclusiva, sin limitar el ingreso al ciberespacio de quienes aún no lo tienen. Sumado a lo anterior, entre los usuarios actuales de Internet existen algunos especialmente vulnerables a los ciberataques, por razones de género, etnia, edad, educación, poder adquisitivo u otras variables que los dejan en una situación de especial atención para el desarrollo de políticas al respecto.

Por los motivos expuestos, es necesario formular una política nacional de ciberseguridad que desde una perspectiva de política pública incorpore en sus procesos críticos niveles de seguridad en el ciberespacio según estándares internacionales.

Ello constituye un desafío que ha sido planteado a nivel internacional, por ejemplo en la OCDE, —entidad en la cual Chile es miembro pleno— se ha hecho particular referencia al desafío para cada uno de los países que forman parte de esta agrupación, consistente en crear una cultura de ciberseguridad que sea parte integral de la rutina diaria de las personas, las empresas y el gobierno en el uso de las tecnologías de la información y la comunicación y en la realización de sus actividades en el entorno digital.[9]

Este desafío tiene implicancias internacionales y nacionales. A nivel internacional, el mayor de ellos es tomar parte en los diversos foros internacionales donde estos temas son discutidos, con fines de

[8] 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".

[9] Disponible en http://www.oecd.org/sti/ieconomy/31670189.pdf

intercambio de información, cooperación y la creación de reglas que fomenten la transparencia y la confianza en torno al uso del ciberespacio, como Naciones Unidas[10], OEA y UNASUR.

A nivel nacional, es el diseño, implementación y puesta en marcha de medidas que permitan proteger la seguridad de los usuarios del ciberespacio. Atendiendo a esta situación y considerando las necesidades nacionales, el programa de Gobierno de la Presidenta Michelle Bachelet contempla **"desarrollar una estrategia de seguridad digital que proteja a los usuarios privados y públicos"[11].** En este sentido, una política de ciberseguridad es necesaria por las siguientes razones:

1. **Resguardar la seguridad de las personas en el ciberespacio**. Es necesario proteger los derechos fundamentales de las personas, especialmente aquellos que dicen relación con sus interacciones en el ciberespacio, tales como la libertad de expresión, el acceso a la información y la protección de la vida privada, así como el patrimonio y la libertad económica, en cuanto a los riesgos propios del ciberespacio como de otras amenazas externas.

2. **Proteger la seguridad del país.** Es necesario resguardar las redes y sistemas informáticos del sector público junto a aquellos componentes del ciberespacio que, independiente de su régimen de propiedad y operación, son esenciales para el adecuado funcionamiento del país. En efecto, es prioritario precisar lo que se desea proteger, es decir, su identificación y el establecimiento de las instituciones que serán parte de la infraestructura crítica de la información. Esto implica considerar los diversos servicios y entidades estratégicas (agua, sistema financiero, energía, defensa, policía, salud, entre otros[12]). Cabe mencionar que este tema tiene dos aristas a considerar: desde la seguridad pública, como también, desde la defensa nacional.

3. **Promover la colaboración y coordinación entre instituciones.** Debido a que las materias involucradas en la ciberseguridad están segmentadas de acuerdo a diversos criterios, observándose la necesidad de generar instancias de comunicación entre diferentes instituciones, organizaciones y empresas tanto públicas como privadas. Por lo tanto, se requiere promover la colaboración, coordinación y sinergia de todos los organismos involucrados en la seguridad en el ciberespacio en sus múltiples dimensiones, bajo una óptica sistémica y progresiva.

4. **Gestionar los riesgos del ciberespacio**. La ciberseguridad va más allá de la protección de la información (acceso, uso, revelaciones, interrupciones, modificaciones o destrucciones no permitidas), también contempla el desarrollo de un proceso de análisis y gestión de riesgos relacionados con la identificación de vulnerabilidades y amenazas en el uso, procesamiento, almacenamiento y transmisión de la información, junto a la generación de una capacidad para recuperarse en caso ser afectado por un ciberataque.

[10] Documento OCDE DSTI/ICCP/REG(2014). A nivel ONU, la discusión específica se remonta al año 1998, con resolución adoptada por la Asamblea General y la creación de 4 grupos de expertos gubernamentales a la fecha. Hoy en día, presenta alto nivel de desarrollo en múltiples foros internacionales, cuya máxima expresión son las Conferencias del ciberespacio: Londres, Budapest, Seúl y el 2015 en La Haya (Holanda). Sumado a lo anterior, a nivel ONU también existen otras instancias como el Foro de Gobernanza de Internet y la Unión Internacional de Telecomunicaciones, donde se discuten temas de ciberseguridad.

[11] Programa de Gobierno de Michelle Bachelet, página 57

[12] "Estudio para la definición e identificación de infraestructura critica de la información en Chile". Elaborado por Zagreb Consultores para la Subsecretaria de Telecomunicaciones de Chile. 2008. Disponible en http://www.subtel.gob.cl/images/stories/articles/subtel/asocfile/infraestructura_critica_020309_v1.pdf

5. Ejes de la Política Nacional de Ciberseguridad

Los siguientes ejes agrupan las diversas medidas que, de acuerdo a estándares internacionales, suelen implementarse en el marco de políticas de ciberseguridad y que son necesarios de acuerdo a la realidad nacional:

1. Infraestructura de la información

- Definir enfoque de gestión de riesgo
- Identificar infraestructuras críticas de la información
- Crear mecanismos de reportes de incidentes
- Definir requisitos y estándares de seguridad (a partir de la asociación público-privada)
- Establecer medidas para enfrentar un incidente (antes, durante y después)
- Diseñar planes de contingencia en ciberseguridad

2. Prevención y sanción

- Definir capacidades de levantamiento, estandarización e integración de datos e información relacionados con el cibercrimen
- Señalar desafíos en los ámbitos de prevención, detección y sanción del cibercrimen
- Aumentar capacidad para investigar y generar evidencia respecto a cibercrímenes
- Diseñar mecanismos de resguardo de derechos fundamentales en la prevención y sanción del cibercrimen

3. Sensibilización, formación y difusión

- Promover una cultura de ciberseguridad a nivel escolar, universitario, como también en los funcionarios públicos y la sociedad civil.
- Fomentar la investigación y desarrollo (I+D) para la seguridad en el ciberespacio orientada a generar capacidad tecnológica propia, de acuerdo a las necesidades nacionales.
- Generar y promover programas de capacitación, educación y formación profesional a nivel de pre y posgrado en materia de ciberseguridad, focalizándose en diferentes objetivos de acuerdo al público objetivo.

4. Cooperación y relaciones internacionales

- Identificar y promover la postura de Chile en la comunidad internacional en materia de ciberseguridad.
- Participar en foros internacionales (Meridian, Octopus, OEA, UNASUR, UIT, IGF, Grupos de expertos ONU, entre otros).
- Analizar la suscripción e implementación de acuerdos internacionales relacionados (Budapest, entre otros).
- Impulsar medidas de cooperación en investigación y asistencia técnica con otros países.

5. Institucionalidad de la ciberseguridad

- Revisar el sistema nacional de ciberseguridad
- Definir roles, atribuciones y competencias de las partes involucradas
- Impulsar mecanismos de intercambio de información
- Crear una alianza público-privada para la seguridad
- Aumentar la capacidad nacional de respuesta a incidentes
- Potenciar equipos de Respuesta ante Emergencias Informáticas (CSIRT)

6. Plan de trabajo

El desarrollo de la PNCS se realizará por medio de una Comisión de Trabajo Interministerial (CTI). Se propone que la institucionalización de esta instancia sea través de un Decreto Supremo que establecerá una Presidencia (por parte del MISP) y una Secretaría Ejecutiva (MDN). En este sentido, el rol de la Secretaría Ejecutiva será coordinar las sesiones de trabajo correspondientes a cada eje temático para la elaboración del documento final de la PNCS.

La SE podrá trabajar junto a otra institución corresponsable con el objetivo dar soporte a la especificidad de materias técnicas. Las reuniones de los grupos de trabajo serán secuenciales y se estima que el inicio será en el mes de abril. Ver esquema N°1 "Trabajo CTI sobre PNCS".

Al respecto, la Secretaría Ejecutiva se encargará de elaborar un documento denominado "términos de referencia" para cada eje temático que será entregado al grupo de trabajo, con el objetivo de introducir y orientar el desarrollo de los contenidos a tratar.

En relación a las sesiones y los productos esperados, es necesario precisar los siguientes aspectos:

1. La discusión por cada eje se realizará en un plazo de seis semanas, desarrollándose al menos tres reuniones por cada eje.
2. En la primera sesión de cada mesa, se presentará la programación del trabajo a desarrollar. Posteriormente en la misma sesión, el documento "términos de referencia", entregado previamente, será comentado y servirá de insumo junto a los aportes que los asistentes entreguen en esta sesión para la elaboración del diagnóstico del tema que aborda cada mesa. Ello será de utilidad para establecer los objetivos del eje en el marco de la PNCS. También serán identificadas las propuestas de acción necesarias para dar cumplimiento a los objetivos formulados en cada eje.
3. En el marco de lo conversado en la primera sesión, las instituciones participantes podrán hacer una estimación del presupuesto que deben considerar en materia de ciberseguridad para el año 2016 y consignarlo en la programación que deberán entregar a sus respectivas autoridades.
4. En la segunda sesión de cada eje, se invitará a exponer a diversas instituciones y/o actores relevantes relacionados con el área y consultar aspectos específicos de interés para el grupo de trabajo.
5. En la tercera sesión se dará a conocer el borrador del informe final del grupo de trabajo del respectivo eje temático.
6. En caso de que el grupo de trabajo lo requiera y con el acuerdo de la Secretaría Ejecutiva es posible convocar a una sesión adicional de trabajo cuando se estime necesario.
7. La versión final de los informes elaborados por de cada eje temático será recibida y consolidada por la Secretaría Ejecutiva.
8. Una vez finalizadas las sesiones, será necesario definir un mecanismo de consulta con otros actores, con el objeto de socializar y legitimar el trabajo realizado.
9. A base de los informes finales y de las consultas realizadas, la Secretaría Ejecutiva procederá a la redacción de la versión final de la PNCS, para su sanción formal por parte de la autoridad, su lanzamiento público y dar paso a la implementación de la política.

Esquema N°1 "Trabajo CTI sobre PNCS"

7. Glosario

- **Ciberespacio:** es un ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior.

- **Ciberseguridad:** es tanto una condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, como el conjunto de políticas y técnicas destinadas a lograr dicha condición.

- **Ciberconflicto:** es la expresión de intereses contrapuestos, entre dos o más partes, en relación a temas, intereses o valores que se manifiestan en el ciberespacio.

- **Ciberataque:** es una expresión del ciberconflicto consistente en acciones hostiles desarrolladas en el ciberespacio con el objetivo de irrumpir, explotar, denegar, degradar o destruir la infraestructura tecnológica, componente lógico o interacciones de éste y pueden tener distintos niveles según su duración, frecuencia y daño generado.

- **Ciberdefensa:** el término posee dos acepciones. (A) En un sentido amplio, son acciones contempladas en el marco de una política nacional de ciberseguridad orientadas a proteger el ciberespacio ante cualquier acción que pueda dañarlo. (B) En un sentido restringido, es el conjunto de políticas y técnicas de la Defensa Nacional destinadas a enfrentar los riesgos y amenazas propias del ciberespacio, de acuerdo con sus atribuciones constitucionales y legales.

- **Cibercrimen:** son los actos delictuales donde el ciberespacio es el objeto del delito o su principal herramienta para cometer ilícitos contra individuos, organizaciones, empresas o gobiernos.

- **Componentes lógicos de la información:** los componentes lógicos de la información corresponden a la capa abstracta de datos que fluyen a través de las infraestructuras físicas de la información. Son componentes lógicos de la información, todos los programas computacionales, los protocolos técnicos de transmisión y almacenamiento de datos en todas sus capas, y en general todas las infraestructuras lógicas que sustentan las interacciones humanas en el ciberespacio.

- **Sistema informático:** todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

- **Dato informático:** toda representación de hechos, información o conceptos expresados de cualquier forma que se presente a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

- **Delito informático:** comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atentar contra la seguridad de los sistemas informáticos o los datos procesados por ellos.

- **Incidente informático:** evento que afecta la confidencialidad, integridad o disponibilidad de la información, como también la continuidad del servicio proporcionado por los sistemas que la contienen.

- **Infraestructura crítica de la información:** 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 salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados.

8. Cronograma de trabajo

2015-2016	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Ene	Feb	Mar
Entrega documento base a autoridades	x												
Preparación términos de referencia	x												
Sesiones GT de ejes temáticos		x	x	x	x	x	x	x					
Entrega informes de GT									x				
Redacción de primera versión									x				
Revisión de primera versión borrador										x			
Socialización											x		
Preparación y entrega versión final												x	
Diseño, edición e impresión												x	
Presentación a la comunidad por autoridad													x