DIARIO OFICIAL
DE LA REPUBLICA DE CHILE
Ministerio del Interior y Seguridad Pública

I SECCIÓN

LEYES, REGLAMENTOS, DECRETOS Y RESOLUCIONES DE ORDEN GENERAL

Núm. 42.003 | Viernes 9 de Marzo de 2018 | Página 1 de 6

Normas Generales

CVE 1363153

MINISTERIO DE DEFENSA NACIONAL

APRUEBA POLÍTICA DE CIBERDEFENSA

Núm. 3.- Santiago, 9 de noviembre de 2017.

Vistos:

1. Las facultades establecidas en el artículo 32, número 6º de la Constitución Política de la República de Chile;
2. La Ley Nº 20.424, Orgánica del Ministerio de Defensa Nacional;
3. Lo preceptuado en el decreto supremo Nº 248, de 29 de noviembre de 2010, que aprueba reglamento orgánico y de funcionamiento del Ministerio de Defensa Nacional;
4. Lo establecido en el decreto supremo Nº 533/2015, de 27 de abril de 2015, que crea el Comité Interministerial sobre Ciberseguridad;
5. Lo ordenado en el Instructivo Presidencial Nº 1/2017, de 27 de abril de 2017, que aprueba e instruye la implementación de la Política Nacional de Ciberseguridad;
6. Lo establecido en la Orden Ministerial Nº 2, de 9 de octubre de 2015, del Ministro de Defensa Nacional, que dispone iniciar el proceso de elaboración de una Política de Defensa en materias de ciberespacio;
7. Lo propuesto por la Subsecretaría de Defensa, y;

Considerando:

1. Que la ley Nº 20.424 establece que le corresponderá al Ministro de Defensa Nacional proponer a la Presidenta de la República la política de defensa nacional y la documentación de la planificación primaria de la Defensa Nacional;
2. Que la ley Nº 20.424 establece que le corresponderá al Subsecretario de Defensa sugerir al Ministro de Defensa Nacional la política de defensa nacional y la planificación primaria de la defensa nacional, así como su actualización y explicitación periódica;
3. Que atendido el desarrollo tecnológico y la creciente incorporación de tecnologías de la información y las comunicaciones en los procesos cotidianos y críticos de la Defensa Nacional, resulta necesario adaptar y actualizar las disposiciones de la política de defensa y los contenidos de la planificación vigente, adecuándolas a este nuevo contexto para una mejor seguridad y defensa nacional;
4. Que el creciente uso de tecnologías de la información y las comunicaciones suponen el surgimiento de nuevos riesgos y amenazas para la seguridad del país, sus habitantes y sus infraestructuras, los cuales deben ser abordados de manera integral;
5. Que, para ello, se aprobó e instruyó la implementación de la Política Nacional de Ciberseguridad, que tiene por objeto esencial resguardar la seguridad de las personas y de sus derechos en el ciberespacio y plantea además cinco objetivos estratégicos de largo plazo, destinados a abordar los múltiples desafíos que enfrenta nuestro país, y un conjunto de medidas de política pública;
6. Que una de las medidas urgentes de la Política Nacional de Ciberseguridad consiste en el establecimiento de una Política de Ciberdefensa que fije los objetivos a ser cumplidos gradualmente hasta el año 2022 por las instituciones de la Defensa Nacional en este ámbito;
7. Que el presente instrumento configura la respuesta del Estado de Chile a los nuevos riesgos y amenazas que el ciberespacio genera para las capacidades de la Defensa Nacional, las cuales incluyen, entre otros elementos, la información, infraestructura y operaciones de defensa;
8. Que, asimismo, esta política forma parte de la Política de Defensa y, por tanto, sostiene los mismos principios básicos que tienen plena expresión en el ciberespacio: el respeto del

derecho internacional público, incluyendo la abstención del uso y la amenaza del uso de la fuerza, la legítima defensa, y el respeto a la soberanía; la promoción de la democracia y el respeto a los derechos humanos; y la protección de la población, de los intereses nacionales, y de la integridad territorial; y,

9. Que, finalmente, la Política de Ciberdefensa constituye un esfuerzo por promover la implementación de medidas de transparencia y generación de confianzas en el sector de la defensa en la región, que son imprescindibles para la mantención de la paz y la seguridad.

Decreto:

Artículo primero. Apruébase la Política de Ciberdefensa del Estado de Chile, cuyo texto será el siguiente:

"POLÍTICA DE CIBERDEFENSA

1. Introducción

Chile, como el resto de América Latina, ha avanzado rápidamente en la incorporación de nuevas tecnologías de información y comunicaciones, tanto en las actividades privadas como en el sector público. Hoy buena parte de los aspectos cotidianos del trabajo, transporte, alimentación, salud y bienestar de las personas dependen del buen funcionamiento de diversos sistemas digitales y de un ciberespacio que los interconecta.

En la última década el país ha sido testigo privilegiado del mayor proceso de innovación tecnológica de la economía mundial, la que se dirige con mucha rapidez a la masificación de la Internet de las Cosas, del Big Data, de la automatización de procesos industriales y el desarrollo de sistemas autónomos letales, entre otras tecnologías emergentes.

Estos sistemas, de complejidad y conectividad crecientes, no son infalibles. Diversas empresas y Estados han sufrido ataques o incidentes en los cuales ha sido comprometida su seguridad, la de sus redes y servicios, afectando con ello el bienestar de las personas. Esta creciente dependencia y vulnerabilidad exige contar con una Política de Estado que permita hacer frente a estos nuevos riesgos y amenazas.

Como respuesta, la Presidenta de la República aprobó el 27 de abril de 2017, la Política Nacional de Ciberseguridad, primer instrumento del Estado de Chile que fija la carta de navegación sobre las medidas que se deben adoptar, tanto en el sector público como en el privado, para contar con un ciberespacio libre, abierto, seguro y resiliente. La Política tiene por objeto esencial resguardar la seguridad de las personas y de sus derechos en el ciberespacio y plantea además cinco objetivos estratégicos de largo plazo, destinados a abordar los múltiples desafíos que enfrenta nuestro país, y un conjunto de medidas de política pública que deben ser implementadas en el corto tiempo. La presente Política de Ciberdefensa es una de las medidas urgentes de adoptar.

La Política de Ciberdefensa forma parte de la Política de Defensa y, por tanto, sostiene los mismos principios básicos: el respeto del derecho internacional público, incluyendo la abstención del uso y la amenaza del uso de la fuerza, la legítima defensa, y el respeto a la soberanía; la promoción de la democracia y el respeto a los derechos humanos; y la protección de la población, de los intereses nacionales, y de la integridad territorial. Todos estos principios tienen plena expresión en el ciberespacio. Chile es un país respetuoso de las normas del Derecho Internacional, que considera completamente aplicables al ciberespacio, el cual debe ser protegido de la misma manera que el espacio terrestre, marítimo o aéreo.

La Política de Ciberdefensa constituye, además, un esfuerzo por promover la implementación de medidas de transparencia y generación de confianzas en el sector de la defensa en la región, que son necesarias para la mantención de la paz y la seguridad.

La Política de Ciberdefensa forma parte de un sistema nacional de políticas digitales, que incluye la Agenda Digital 2020, la mencionada Política Nacional de Ciberseguridad y la Política Internacional para el Ciberespacio. La Política de Ciberdefensa complementa a la de Ciberseguridad en aquellos aspectos relacionados directamente con la defensa de la soberanía del país a través de las redes digitales, con la protección de nuestra infraestructura crítica de información, y con la protección de los derechos humanos de todas las personas que habitan en nuestro territorio.

La presente Política fija los objetivos a ser cumplidos gradualmente hasta el año 2022, y requerirá que las instituciones de la Defensa Nacional avancen en su implementación, incluyendo actividades en su planificación de corto, mediano y largo plazo.

2. Diagnóstico

La Política de Ciberdefensa constituye una respuesta a los nuevos riesgos y amenazas que el ciberespacio genera para las capacidades de la Defensa Nacional, las cuales incluyen, entre otros elementos, la información, la infraestructura y las operaciones de defensa.

El uso intensivo de tecnologías de la información en el diseño, desarrollo y ejecución de una multiplicidad de procesos cotidianos y críticos de cada una de las instituciones y organismos del sector de la Defensa Nacional, han incrementado el nivel de dependencia y vulnerabilidad propia de estas tecnologías, que deben ser abordados de manera sistémica y con enfoque en la gestión de riesgos.

En la última década se ha incrementado el número de ataques digitales que han recibido las instituciones del sector defensa, las que pueden caracterizarse como de baja y mediana intensidad; y se proyecta un aumento constante de este tipo de amenazas en el futuro. Asimismo, ha aumentado tanto el nivel de sofisticación de éstos como el nivel de daño que pueden llegar a provocar, variando desde la denegación de servicios masivos (DDoS) hasta la utilización de malware especialmente desarrollado y ataques de fuerza bruta contra servidores institucionales, siendo incluso susceptible de ser afectada la capacidad de defensa por incidentes de seguridad de carácter global no dirigidos, como el ransomware WannaCry, de mayo de 2017.

Desde un punto de vista de seguridad internacional, los conflictos internacionales también pueden manifestarse en el ciberespacio, y lo hacen de múltiples maneras. Dentro de este contexto, se presentan nuevos desafíos para la comunidad internacional, entre los que se encuentran el carácter global y transfronterizo del ciberespacio, la creciente cantidad y tipo de ciberataques, la dificultad de atribuir el origen de éstos y la creciente ubicuidad con que se presentan, debido al crecimiento exponencial de dispositivos conectados a la red.

Todo ello hace imprescindible contar con un instrumento de política pública normativo para la planificación y empleo de la Defensa Nacional en materia de ciberdefensa y asegure el cumplimiento del mandato constitucional de protección de la seguridad exterior del país, en este ámbito.

3. Principios de la Defensa Nacional y su aplicación al ciberespacio

La Defensa Nacional sitúa su política de ciberdefensa dentro del marco jurídico institucional vigente en el país, y reconoce y respeta los tratados y acuerdos internacionales suscritos, aprobados y ratificados por Chile, sus normas, principios y costumbres. Consecuentemente, la política de ciberdefensa se enmarca dentro de los siguientes lineamientos generales o principios:

3.1. La Política de Ciberdefensa forma parte del esfuerzo del Estado por ofrecer seguridad a todos los habitantes, generando las condiciones para que puedan hacer un uso pacífico, equitativo y seguro del ciberespacio, y estableciendo tanto las regulaciones para el ejercicio de sus derechos como el marco de conducta para se lleven a cabo dichas actividades. La Política de Ciberdefensa es parte de la Política Nacional de Ciberseguridad, en especial en los siguientes aspectos:

- La Política de Ciberdefensa contribuye al logro del objetivo de contar con una infraestructura de la información robusta y resiliente en el sector de la Defensa Nacional, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una perspectiva de gestión de riesgos;
- La Política de Ciberdefensa se formula y ejecuta dentro del marco de respeto a los derechos de las personas en el ciberespacio;
- La ciberdefensa se desarrolla en coherencia con la cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales que defina el Estado para el conjunto de los actores nacionales;
- La ciberdefensa contribuye al objetivo de prevenir que desde Chile se lleven a cabo acciones ilícitas en contra de otros Estados, sus habitantes o sus intereses, en el ámbito de competencia de la Defensa Nacional.

3.2. La Política de Ciberdefensa es parte de la Política de Defensa Nacional, y forma parte integral de los objetivos y principios de éstas, en especial en lo referido a:

- Las operaciones de defensa en el ciberespacio constituyen una dimensión específica del espectro contemporáneo del empleo de las capacidades de defensa.

- La planificación, conducción y ejecución de las operaciones en el ciberespacio se ceñirá estrictamente al respeto del Derecho Internacional Público, con especial consideración al Derecho Internacional de los Derechos Humanos y al Derecho Internacional Humanitario. Por tanto, Chile se abstendrá de recurrir a la amenaza de uso o al uso de la fuerza en una forma que contravenga el Derecho Internacional y podrá hacer uso de la fuerza en legítima defensa en el ciberespacio, de conformidad con lo dispuesto en el artículo 51 de la Carta de Naciones Unidas.

- Chile promoverá en el ciberespacio la cooperación para mantener la paz y la seguridad internacional.

3.3. La Política de Ciberdefensa requiere de una estrecha colaboración con otros actores de la institucionalidad del Estado.

Esa colaboración se materializa a través de la participación en las diversas instancias que establece esa institucionalidad para la toma de decisiones, en relación con la formulación, ejecución y control de políticas, planes, programas y acciones en la materia, así como en el intercambio y colaboración en el plano técnico y operacional.

La colaboración en el trabajo y acción en materias de ciberdefensa se materializará de forma integral con otros sectores del país, con entidades privadas, y con la sociedad civil.

3.4. La Política de Ciberdefensa requiere para su eficacia de una intensa cooperación con otros actores equivalentes en el plano internacional, preservándose en lo que corresponda a la seguridad operacional de las capacidades del país.

La cooperación internacional es imprescindible para contar con un ciberespacio libre, abierto y seguro, sobre la base de una regulación internacional democrática, que preserve los derechos de las personas y regule la conducta de los Estados en esta dimensión.

La Política de Ciberdefensa es coadyuvante de la Política Exterior, y materializa el principio de responsabilidad de cooperar que ésta establece. Por ello, y en coordinación con el Ministerio de Relaciones Exteriores, se impulsarán relaciones de cooperación en ciberseguridad y ciberdefensa con otros actores estatales, y se participará activamente en foros y discusiones internacionales pertinentes.

3.5. La Política de Ciberdefensa reconoce que el desarrollo tecnológico en materia de tecnologías de la información es decisivo y crítico para el desarrollo y empleo de las capacidades, tanto en la dimensión digital como cinética.

La Política de Ciberdefensa y la Política Nacional de Ciberseguridad orientarán en lo sucesivo la política militar en aquellos aspectos o factores de desarrollo de capacidades en materia digital. En particular, es orientadora de una política de la industria de la Defensa Nacional, proveedora de bienes y servicios en el ámbito de las tecnologías de la información. El Ministerio de Defensa Nacional promoverá el desarrollo de una industria que sirva a los objetivos estratégicos para la Defensa Nacional, y que le permita mantener un adecuado nivel de independencia y soberanía tecnológica.

4. Políticas de la Defensa Nacional y su aplicación al ciberespacio

4.1. Sobre el empleo de los medios de ciberdefensa.

El Estado de Chile considera que un ciberataque puede llegar a ser tan dañino como un ataque armado. Chile podrá considerar los ciberataques masivos sobre su soberanía, sus habitantes, su infraestructura, o aquellos que afecten gravemente sus intereses, como un ataque armado, y de acuerdo con el artículo 51 de la Carta de las Naciones Unidas, podrá hacer uso de los medios que estime apropiados, tanto físicos como digitales, en el ejercicio de su derecho a la legítima defensa.

El Estado de Chile protegerá su infraestructura crítica de la información, ejerciendo su soberanía sobre aquellas redes y recursos digitales. La Defensa Nacional se ocupará de identificar la ocurrencia de ataques, facilitar o permitir su correcta atribución a otros Estados o grupos no estatales, aplicar las contramedidas adecuadas, y dar cumplimiento a la obligación internacional de identificar y detener los ataques que otros países puedan realizar a través de su infraestructura de información.

4.2. Cooperación internacional y promoción de la transparencia y la confianza entre los Estados.

Atendido el carácter transfronterizo del ciberespacio, una de las mejores formas de enfrentar los riesgos y amenazas que su uso intensivo genera es establecer relaciones de cooperación en ciberdefensa con otros actores estatales, organismos internacionales y participar de manera activa en foros y discusiones internacionales, que propenden a generar un ciberespacio seguro en el ámbito de la defensa. El ciberespacio también se encuentra regido por el derecho internacional, y

el desafío es interpretar las disposiciones vigentes de los diversos acuerdos internacionales, en consonancia con los principios de política exterior de Chile.

La Defensa Nacional participará activamente en la elaboración y posterior implementación de las medidas de transparencia y de generación de confianza, discutidas y promovidas tanto bilateralmente como en diversos foros internacionales multilaterales, políticos y militares, tales como la Organización de Naciones Unidas, la Organización de Estados Americanos, y el Consejo de Defensa Suramericano de la Unión de Naciones Sudamericanas, entre otros.

Chile promoverá tanto una conducta en el ciberespacio basada en los principios antes señalados, como la adopción de códigos de conducta y de normas internacionales que fomenten la paz y la seguridad internacional, particularmente a nivel regional y con sus países vecinos.

4.3. Desarrollo de capacidades.

El Estado de Chile desarrollará y mantendrá las capacidades técnicas necesarias para resguardar la confidencialidad, la integridad y la disponibilidad del ciberespacio institucional del sector Defensa, con especial atención, al menos, a sus i) Sistemas y redes de comunicaciones institucionales; ii) Sistemas y redes de mando y control; y, iii) Sistemas de armas.

El objetivo es contar con un ciberespacio institucional robusto y resiliente que sea capaz de enfrentar y hacerse cargo de los riesgos y amenazas digitales que puedan afectar su confidencialidad, integridad y disponibilidad.

El Estado de Chile desarrollará y mantendrá las capacidades necesarias para la autodefensa del país -en conformidad con la Política Nacional de Ciberseguridad-, y la protección de sus intereses vitales, para lo cual se requiere no sólo de los recursos y herramientas técnicas pertinentes, sino que exige contar con personal calificado, en número y aptitudes suficientes, en todos los niveles institucionales, mediante programas generales y especializados de formación, capacitación y sensibilización del personal del sector de la Defensa Nacional y sus entornos más cercanos.

Para ello, el Ministerio de Defensa Nacional y sus instituciones dependientes y relacionadas deberán, de conformidad con la legislación vigente:

a. Identificar y definir el rol del recurso humano en la ciberdefensa;

b. Implementar los modelos formativos que sean necesarios para cumplir con ese rol;

c. Definir y crear las especialidades, subespecialidades o especialidades secundarias en el área de la ciberdefensa para oficiales y suboficiales, manteniendo una continuidad de trabajo en dicha área de desempeño, reestudiando los requisitos de ascenso y otras obligaciones o interferencias que pudieran afectar su continuidad como especialistas. Se deberá considerar y promover la igual participación de mujeres y hombres en el área de la ciberdefensa;

d. Identificar e implementar modelos de reclutamiento y reserva de personal calificado;

e. Incrementar la interacción con el sector privado y académico, para contar con sus capacidades en la materia; y

f. Promover la innovación y la investigación aplicada en materia de ciberseguridad, desde una perspectiva conjunta.

La ciberdefensa ha impuesto retos que deben ser afrontados institucionalmente. Para ello, la Defensa Nacional realizará la reorganización orgánica que sea necesaria para el cumplimiento de sus funciones en el ciberespacio, que comprenda, al menos, las siguientes medidas:

a. Se creará un Comando Conjunto de Ciberdefensa, bajo el mando del Jefe del Estado Mayor Conjunto, responsable del planeamiento y ejecución de las operaciones militares conjuntas de ciberdefensa del país;

b. Se creará un Equipo de Respuestas a Incidentes Informáticos (CSIRT) de la Defensa Nacional, que junto con brindar seguridad a las redes y sistemas del Ministerio de Defensa Nacional, actuará como ente coordinador técnico con los CSIRT de las instituciones de la Defensa Nacional, el que será dirigido por el Estado Mayor Conjunto. En el mediano plazo se implementará un CSIRT sectorial que coordine los CSIRT institucionales;

c. Cada rama de las Fuerzas Armadas contará con un CSIRT, y se evaluará la necesidad de crear nuevos equipos en los organismos relacionados o dependientes del Ministerio de Defensa Nacional;

d. Se creará una Oficina de Ciberdefensa y Seguridad de la Información en el Gabinete del Ministro de Defensa Nacional, que tendrá por función esencial prestar asesoría en materia de ciberseguridad y ciberdefensa;

e. Se fortalecerán las capacidades de ciberseguridad del Ministerio de la Defensa Nacional y sus instituciones dependientes o relacionadas; y

f. Se creará una capacidad de reserva nacional para la ciberdefensa del país.

5. Instrumentos de la Política de Ciberdefensa

5.1. La Subsecretaría de Defensa elaborará un plan para la implementación de la Política de Ciberdefensa, con participación de los demás organismos e instituciones del sector de la Defensa Nacional.

5.2. Se desarrollarán y establecerán normas y regulaciones para el cumplimiento de la misión de la Defensa Nacional en el ciberespacio:

a. La Subsecretaría de Defensa propondrá las interpretaciones de las normas que rigen los conflictos armados y el derecho internacional humanitario, para su aplicación en el ciberespacio, en coordinación con el Ministerio de Relaciones Exteriores.

b. La Subsecretaría de Defensa propondrá los objetivos políticos del empleo de los medios de ciberdefensa, en el marco de la planificación de la Defensa que le compete.

c. La Subsecretaría para las Fuerzas Armadas propondrá una política informática del Ministerio de Defensa Nacional, acorde a los lineamientos de la Política de Ciberdefensa.

d. La Subsecretaría para las Fuerzas Armadas diseñará un marco operacional que garantice el respeto y promoción de los derechos humanos y del derecho internacional aplicable.

e. El Estado Mayor Conjunto propondrá la doctrina de empleo conjunto de los medios de ciberdefensa y la planificación estratégica conjunta de los mismos. Asimismo, el Estado Mayor Conjunto verificará la correspondencia de la doctrina y planificación institucional con la doctrina y planificación conjunta.

f. Las Fuerzas Armadas prepararán la doctrina y planificación estratégica de empleo institucional de los medios de ciberdefensa.

5.3. La presente Política de Ciberdefensa será revisada cada cuatro años, o cuando las circunstancias lo ameriten, en un proceso dirigido y coordinado por la Subsecretaría de Defensa.

6. Glosario

Ciberataque: Una operación o actividad en el ciberespacio, ya sea ofensiva o defensiva, que se espera que cause heridas o muerte a personas, o daño o destrucción de objetos.

Ciberdefensa: Conjunto de principios, políticas e instrumentos destinados a proteger el ciberespacio desde un punto de vista de la defensa nacional y estratégico-militar.

Ciberespacio: Conjunto de las infraestructuras físicas, lógicas y las interacciones que ahí se producen.

Ciberseguridad: 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 también el conjunto de políticas y técnicas destinadas a lograr dicha condición.

Infraestructura de la información: Aquella infraestructura conformada por las personas, procesos, procedimientos, herramientas, instalaciones y tecnologías que soportan la creación, uso, transporte, almacenamiento y destrucción de la información.

Infraestructuras críticas 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 seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado.

Artículo segundo. El gasto que genere la ejecución de la Política de Ciberdefensa deberá ser asumido por las respectivas instituciones responsables de su implementación y deberá ser incorporado en sus presupuestos institucionales anuales, salvo aquellas medidas que formen parte de la ejecución de proyectos de inversión financiados con cargo a la ley Nº 13.196.

Anótese, tómese razón, comuníquese y publíquese en el Diario Oficial y en el Boletín Oficial del Ejército de Chile, Armada de Chile y Fuerza Aérea de Chile.- MICHELLE BACHELET JERIA, Presidenta de la República.- José Antonio Gómez Urrutia, Ministro de Defensa Nacional.

Lo que transcribo para su conocimiento.- Marcos Robledo Hoecker, Subsecretario de Defensa.