Nueva normativa sobre ciberseguridad en Chile

La Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información y su relación con otras normas y políticas

DERECHOS DIGITALES
América Latina

Esta publicación fue creada por Derechos Digitales, una organización independiente sin fines de lucro, fundada en 2005, que tiene como misión la defensa, promoción y desarrollo de los derechos humanos en entornos digitales en América Latina.

Supervisión general: Michel Souza y J. Carlos Lara
Redacción: Valentina Arriagada Alvarado
Edición: J. Carlos Lara
Diseño: Catalina Viera

Marzo / Noviembre, 2024.

Esta publicación fue posible gracias al apoyo de Global Partners Digital.

Valentina Arriagada Alvarado es abogada de la Universidad de Chile, ayudante del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile. Contacto: valentina.arriagada@derecho.uchile.cl

Índice

Resumen Ejecutivo

La nueva Ley Marco de Ciberseguridad de Chile, promulgada el 26 de marzo de 2024 por el Presidente de la República y diez ministros y ministras de estado,[1] establece una regulación integral que busca hacer frente a los desafíos en materia de ciberseguridad, incluyendo la prevención de ciberataques, el establecimiento de una gobernanza e institucionalidad robustas, y la promoción de la coordinación entre el sector público y privado.

El presente documento contiene una descripción de la nueva normativa que aborda sus principales disposiciones. Se destacan disposiciones claves que distinguen entre servicios esenciales y operadores de importancia vital, así como las obligaciones, infracciones y sanciones que atañen a cada uno; la creación de la Agencia Nacional de Ciberseguridad y la coordinación regulatoria. Asimismo, destaca el catálogo de definiciones y de principios rectores que tendrán un papel importante en la interpretación e implementación de la ley en todos sus niveles. Por otro lado, se evidencia que la ley marco de ciberseguridad tendrá una notable influencia en otros cuerpos normativos con los que se relacionará continuamente, por lo que ejercerá además un rol de entregar coherencia a las acciones y medidas que atañen a la seguridad de los sistemas informáticos en distintos ámbitos.

En definitiva, en conjunto con la modificación a la Ley Nº 19.628 sobre protección a la vida privada, aún en trámite en el Congreso a la fecha de publicación de la Ley Marco, y con la reciente ley de delitos informáticos, la nueva regulación representa un hito al poner a Chile en la vanguardia en materia de regulación en ciberseguridad en la región, que permitiría avanzar en la construcción de un ciberespacio libre, abierto, seguro y resiliente.

[1] El 26 de marzo de 2024 la Ley Marco de Ciberseguridad fue promulgada por el Presidente de la República, Gabriel Boric Font, y por sus ministros y ministras de los ministerios del Interior y Seguridad Pública; Relaciones Exteriores; Defensa Nacional; Hacienda; Secretaría General de la Presidencia; Economía, Fomento y Turismo; Justicia y Derechos Humanos; Transportes y Telecomunicaciones; Energía; y, Ciencia Tecnología, Conocimiento e Innovación. La ley publicada el 8 de abril en el Diario Oficial, como Ley Nº 21.663.

I. Introducción

El desarrollo de un marco legal sobre ciberseguridad e infraestructura crítica de la información fue una de las medidas de la agenda de política pública contemplada en la Política Nacional de Ciberseguridad lanzada en Chile el año 2017.[2]

Varios años más tarde, en un contexto de numerosos ciberataques a diversos organismos como el Estado Mayor Conjunto, el Servicio Nacional del Consumidor y el Poder Judicial,[3] el 15 de marzo del año 2022 ingresó al Senado el proyecto de ley marco sobre ciberseguridad e infraestructura crítica de la información, mediante mensaje del Presidente de la República.

En el mensaje, el Ejecutivo reconoció el permanente riesgo de ciberataques e incidentes de ciberseguridad, y la importancia de ésta en el proceso de adaptabilidad a la sociedad digital. Para lo anterior, se determinó como propósito robustecer la ciberseguridad en Chile, creando la institucionalidad necesaria, fortaleciendo el trabajo preventivo, formando cultura en materia de seguridad digital, enfrentando las contingencias en el sector público privado, y resguardando la seguridad de las personas en el ciberespacio.[4] La institucionalidad a crear está centrada en la denominada Agencia Nacional de Ciberseguridad (en adelante, denominada en forma abreviada como "ANCI").

A casi dos años desde el ingreso del proyecto, la nueva regulación e institucionalidad en materia de ciberseguridad se encuentra convertida en ley, y su implementación supondrá un desafío tanto para los organismos de la Administración del Estado como para las instituciones privadas que se encuentren bajo su ámbito de aplicación.

Este documento busca resumir los principales aspectos que introduce la ley marco de ciberseguridad (en adelante "LMC"), sus principales desafíos y puntos pendientes de forma previa a su reglamentación, y la forma en que se relaciona con otras normas legales, políticas estatales y proyectos de ley.

---

[2] Política Nacional de Ciberseguridad 2017-2022, disponible en: https://digital.gob.cl/biblioteca/estrategias/politica-nacional-de-ciberseguridad-2017-2022/

[3] Jaime Urzúa, "Los ciberataques masivos más importantes de 2022", Diario Constitucional, 2022, disponible en https://www.diarioconstitucional.cl/estudios-juridicos/los-ciberataques-masivos-mas-importantes-de-2022-por-jaime-urzua/

[4] Mensaje de S.E. el Presidente de la República con el que inicia un proyecto de ley marco sobre ciberseguridad e infraestructura crítica de la información, 2 de marzo de 2022, Boletín Nº 14.847-06.

II. La ley marco sobre ciberseguridad e infraestructura crítica de la información

1. Objeto de la LMC

El artículo 1º de la LMC establece por objeto el establecimiento de "la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones determinadas en el artículo 4º, y los mecanismos de control, supervisión y de responsabilidad ante infracciones".

2. Ámbito de aplicación

En su inicio, el proyecto de ley delimitaba su ámbito de aplicación en torno al concepto de "infraestructura crítica de la información", como concepto para distinguir a aspectos especiales dignos de protección. Sin embargo, dicho concepto fue señalado como extremadamente rígido, proponiéndose su modificación por conceptos más modernos.[5] Así, el texto final de la LMC define su ámbito de aplicación en relación con servicios calificados como "esenciales" y los denominados "operadores de importancia vital".

2.1. Servicios esenciales

La LMC será aplicable a las instituciones prestadoras de servicios que se califican como esenciales. El artículo 4º define como servicios esenciales los siguientes:

> i. Los servicios provistos por los organismos de la Administración del Estado[6] y por el Coordinador Eléctrico Nacional;
>
> ii. Los servicios prestados bajo una concesión de servicio público;
>
> iii. Los servicios proveídos por instituciones privadas que realicen alguna de las siguientes actividades: transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento; telecomunicaciones; infraestructura digital; servicios digitales y servicios de tecnología de la información gestionados

[5] "Informe de la Comisión de Seguridad Pública del Senado recaído en el proyecto de ley, en primer trámite constitucional, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información", 12 de octubre de 2022, p. 11.

[6] El artículo 1º de la LMC dispone que, para efectos de esta ley, la Administración del Estado estará constituida por los Ministerios, las delegaciones presidenciales regionales y provinciales, los Gobiernos Regionales, las Municipalidades, las Fuerzas Armadas, de Orden y Seguridad Pública, las empresas públicas creadas por ley, y los órganos y servicios públicos creados para el cumplimiento de la función administrativa. Asimismo, dispone que la ley aplicará a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio.

por terceros; transporte, así como la operación de su infraestructura respectiva; banca, servicios financieros y medios de pago; prestaciones de seguridad social; servicios postales y de mensajería; prestación institucional de salud, y la producción y/o investigación de productos farmacéuticos; y,

iv. Otros servicios que sean calificados como esenciales por la ANCI. En efecto, por resolución fundada del Director o Directora Nacional, la ANCI podrá calificar otros servicios no establecidos en la ley como servicios esenciales, cuando su afectación puede causar un grave daño a la vida o integridad física de la población o a su abastecimiento, a sectores relevantes de las actividades económicas, al medioambiente, al normal funcionamiento de la sociedad y/o de la Administración del Estado, a la defensa nacional, o a la seguridad y el orden público.

2.2. Operadores de importancia vital

Se trata de servicios esenciales que serán calificados como operadores vitales mediante resolución dictada por el Director o Directa Nacional de la ANCI.

Dicha calificación se dará a los servicios esenciales que cumplan con dos requisitos:

i. Que la provisión de dicho servicio dependa de las redes y sistemas informáticos; y,

ii. Que la afectación, interceptación, interrupción o destrucción de sus servicios tenga un impacto significativo en la seguridad y el orden público, en la provisión continua y regular de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado o, en general, de los servicios que éste debe proveer o garantizar.

Es relevante mencionar que la ANCI podrá calificar como operadores de importancia vital (en adelante también señalados como “OIV”) a instituciones privadas que, aunque no tengan la calidad de prestadores de servicios esenciales, reúnan los requisitos antes indicados y cuya calificación sea indispensable por haber adquirido un rol crítico en el abastecimiento de la población, la distribución de bienes o la producción de aquellos indispensables o estratégicos para el país; o por el grado de exposición de la entidad a los riesgos y la probabilidad de incidentes de ciberseguridad, incluyendo su gravedad y las consecuencias sociales y económicas asociadas.

3. Definiciones

El artículo 2º establece una serie de definiciones, que fueron objeto de discusión dentro del debate legislativo. Algunas de las más relevantes incluyen:

Ciberseguridad: preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.

Ciberataque: intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.

Incidente de ciberseguridad: todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.

Riesgo: posibilidad de ocurrencia de un incidente de ciberseguridad; la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias del mismo.

Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

Activo informático: toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.

Red y sistema informático: conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.

Confidencialidad: propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.

Disponibilidad: propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.

Integridad: propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.

Resiliencia: capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.

4. Principios

La LMC establece una serie de principios rectores, los que fueron entendidos en su origen como criterios normativos de aplicación general, con función integradora e interpretativa, que determinan el sentido y alcance de la ley en su conjunto, por lo que orientarán la aplicación de la ley y los actos que ejecute la ANCI y las entidades reguladas.

Así, el artículo 3º de la LMC, con el propósito de alcanzar los objetivos de la ley, establece los principios que se enumeran a continuación:

Control de daños: frente a un ciberataque o a un incidente de ciberseguridad se deberá actuar coordinada y diligentemente, y adoptar las medidas para evitar su escalada y su posible propagación a otros sistemas.

Cooperación con la autoridad: para resolver los incidentes de ciberseguridad se deberá prestar cooperación con la autoridad competente y, si es necesario, cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.

Coordinación: la ANCI y las autoridades sectoriales deberán cumplir sus cometidos coordinadamente, propender a la unidad de acción y evitar la duplicación o interferencia de funciones.

Seguridad en el ciberespacio: es deber del Estado resguardar la seguridad en el ciberespacio y velar que las personas puedan participar de un ciberespacio seguro, por lo que otorgará especial protección a las redes y sistemas que contengan información de aquellos grupos de personas que suelen ser en mayor medida objeto de ciberataques.

Respuesta responsable: la aplicación de medidas para responder a incidentes de ciberseguridad o ciberataques en ningún caso podrá significar la realización o el apoyo a operaciones ofensivas.

Seguridad informática: toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias.

Racionalidad: las medidas para la gestión de incidentes, las obligaciones de ciberseguridad y el ejercicio de las facultades de la ANCI deberán ser necesarias y proporcionales al grado de exposición a los riesgos, y al eventual impacto social y económico.

Seguridad y privacidad por defecto y desde el diseño: los sistemas informáticos, aplicaciones y tecnologías de la información deben diseñarse, implementarse y gestionarse teniendo en cuenta la seguridad y la privacidad de los datos personales que procesan.

5. Obligaciones de ciberseguridad

La aplicación de la LMC está definida según si las entidades obligadas son o no, a su vez, parte de la categoría de operadores de importancia vital. Se distinguen así deberes generales para todas ellas, y deberes específicos para los operadores de importancia vital.

5.1. Deberes generales

De conformidad con lo dispuesto en el artículo 7º de la LMC, todas las entidades obligadas por la ley deberán cumplir con los deberes indicados a continuación:

i. Aplicar de manera permanente las medidas tecnológicas, organizacionales, físicas y/o informativas para prevenir, reportar y resolver incidentes de ciberseguridad.

ii. Implementar protocolos y estándares establecidos por la ANCI.

iii. Implementar estándares particulares dictados conforme a la respectiva regulación sectorial.

Estos protocolos y estándares deben tener por objeto prevenir y gestionar los riesgos asociados a la ciberseguridad, así como contener y mitigar el impacto que los incidentes puedan tener sobre la continuidad operacional del servicio prestado o la confidencialidad y la integridad de la información o de las redes o sistemas informáticos.

5.2. Deberes específicos

Además de los deberes generales, en el artículo 8º de la LMC se establecen los siguientes deberes específicos que deben ser observados por los Operadores de Importancia Vital:

i. Implementar un sistema de gestión de seguridad de la información continuo.

ii. Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de seguridad.

iii. Elaborar e implementar planes de continuidad operacional y ciberseguridad, los cuales deberán certificarse y someterse a revisiones periódicas.

iv. Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y sistemas para detectar acciones o programas informáticos que comprometan la ciberseguridad y comunicar la información relativa a dichas acciones o programas al Equipo Nacional de Respuesta a Incidentes de Seguridad Informática ("CSIRT Nacional").

v. Adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad.

vi. Contar con las certificaciones que la ley establece.

vii. Informar a los potenciales afectados, en la medida que puedan identificarse y cuando así lo requiera la ANCI, sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, especialmente cuando involucren datos personales y no exista otra disposición legal que requiera su notificación; o cuando sea necesario para prevenir la ocurrencia de nuevos incidentes o para gestionar uno que ya hubiera ocurrido.

viii. Contar con programas de capacitación, formación y educación continua de los trabajadores y colaboradores, incluyendo campañas de ciberhigiene.

ix. Designar un delegado de ciberseguridad, quien actuará como contraparte de la ANCI e informará a la autoridad, jefatura, jefe superior, directores o gerentes de la entidad.

5.3. El deber de reportar vulnerabilidades

Un deber adicional es regulado de manera especial. En el artículo 9º, por su relevancia y complejidad, se regula de forma separada a los deberes generales y específicos de la sección anterior, la obligación común a todas las instituciones reguladas por la LMC de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos, tan pronto como les sea posible y conforme al esquema establecido en la ley, con deberes específicos diferenciados si la entidad en cuestión se trata de un operador de importancia vital.

El artículo 27 precisa que se considerarán significativos los incidentes que sean capaces de interrumpir la continuidad de un servicio esencial o afectar la integridad física o la salud de las personas, y en caso de que afecten sistemas informáticos que contengan datos personales.

Los siguientes criterios ayudarán a definir la importancia de los efectos de un incidente:

a. El número de personas afectadas.
b. La duración del incidente.
c. La extensión geográfica con respecto a la zona afectada por el incidente.

6. Institucionalidad

6.1. Agencia Nacional de Ciberseguridad

La LMC trae consigo novedades institucionales, por cuanto, entre otras entidades, crea la Agencia Nacional de Ciberseguridad o ANCI, la que será un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, de carácter técnico y especializado. La ANCI tendrá por objeto asesorar al Presidente de la República en materias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, velar por la protección, la promoción y respeto del derecho a la seguridad informática, y coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

La ANCI estará dirigida por un Director o Directora Nacional, quien será el jefe superior del servicio. Asimismo, existirá un subdirector o subdirectora nacional.

En línea con su objeto, dentro de sus atribuciones se encuentra el prestar asesoramiento al Presidente de la República; dictar protocolos y estándares para las entidades reguladas; aplicar e interpretar administrativamente las disposiciones en la materia; coordinar y supervisar el CSIRT Nacional y a los demás pertenecientes a la Administración del Estado; crear un Registro Nacional de Incidentes; calificar a los servicios esenciales y a los OIV; colaborar con los organismos integrantes del Sistema de Inteligencia del Estado en la identificación de amenazas y la gestión de incidentes o ciberataques que puedan representar un riesgo para la seguridad nacional; fiscalizar el cumplimiento de la ley y normas asociadas; iniciar procedimientos sancionatorios y sancionar infracciones e incumplimientos; y, entre otras, realizar todas aquellas funciones que las leyes le encomienden especialmente.

Además, la ANCI administrará la Red de Conectividad Segura del Estado (“RCSE”), red encargada de proveer servicios de interconexión y conectividad a internet a los organismos de la Administración del Estado.

De acuerdo al artículo 53 de la LMC, la mencionada coordinación y supervisión por la ANCI no alcanzan al Senado y la Cámara de Diputados, el Poder Judicial, la Contraloría General de la República, el Banco Central, el Ministerio Público, el Servicio Electoral ni el Consejo Nacional de Televisión. Así, estos órganos autónomos constitucionales deberán adoptar las medidas de seguridad de sus redes y sistemas informáticos que

sean pertinentes, pero sin estar sujetos a la supervigilancia de la ANCI. Sin perjuicio de lo anterior, deberán convenir mecanismos de reporte de incidentes y de coordinación y cooperación para la respuesta a los mismos.

El artículo 53 aprobado por el Congreso Nacional contemplaba un inciso tercero, según el cual si el órgano autónomo constitucional además se trataba de una autoridad sectorial, debía considerársele para los efectos de los artículos 6º (sobre el pronunciamiento sobre instituciones que deban calificarse como operadores de importancia vital), 25 (sobre coordinación regulatoria entre autoridades sectoriales y la ANCI) y 26 (relativo a la dictación de normativa sectorial sobre ciberseguridad). Sin embargo, este inciso fue declarado inconstitucional en la etapa de control de constitucionalidad de la LMC, pues podría afectar la autonomía constitucional de dichos órganos, al considerar que la norma contraría directamente los artículos 19 Nº 12 inciso sexto; 55; 76; 84; 94 bis; 98; y 108, de la Constitución Política.[7]

6.2. Otras entidades

Además de la ANCI, la LMC instituye otras entidades, y regula por ley algunas ya existentes,[8] la ANCI, la LMC instituye otras entidades, y regula por ley algunas ya existentes, que jugarán un rol específico y relevante en la implementación de la normativa.

> Consejo Multisectorial sobre Ciberseguridad: consejo de carácter consultivo, integrado por el Director o Directora Nacional de la ANCI y seis consejeros ad honorem designados por el Presidente de la República. Tendrá la función de asesorar y formular recomendaciones a la ANCI en el análisis y revisión periódica de la situación de ciberseguridad del país, en el estudio de las amenazas existentes y potenciales en el ámbito de ciberseguridad, y proponer medidas para abordarlas.
>
> Equipo Nacional de Respuesta a Incidentes de Seguridad Informática: el CSIRT Nacional): equipo al interior de la ANCI, que tendrá, entre otras, las funciones de responder ante ciberataque o incidentes cuando sean de efecto significativo; coordinar a los CSIRT que pertenezcan a organismos de administración del estado o a la defensa nacional; servir de punto de enlace entre los equipos de respuesta extranjeros; colaborar o asesorar a los CSIRT de organismos de la Administración del Estado; supervisar incidentes a escala nacional; realizar entrenamiento, educación y capacitación; difundir alertas tempranas, avisos e información sobre riesgos e incidentes para la comunidad.

---

7 Tribunal Constitucional, sentencia Rol Nº 15.043-23, de 19 de marzo de 2024.

8 En efecto, desde antes de la LMC ha existido el Equipo Nacional de Respuesta de Seguridad Informática de Gobierno como un Departamento bajo la División de Redes y Seguridad Informática, al interior de la Subsecretaría del Interior y Seguridad Pública, formalizado por Resolución Exenta Nº 5.006 de 2019. Con la LMC este equipo pasa a ser parte de la ANCI. De igual manera, la LMC regula a nivel legal el Comité Interministerial sobre Ciberseguridad, el cual fue creado por Decreto Supremo Nº 533 de 2015 del Ministerio del Interior y Seguridad Pública.

Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional: organismo dependiente del Estado Mayor Conjunto, del Ministerio de Defensa Nacional, que será el responsable de la coordinación, protección y seguridad de las redes y sistemas de dicho Ministerio y de los servicios esenciales y operadores vitales para la defensa nacional, además de cumplir aquellas tareas que le sean encomendadas.

Comité Interministerial sobre Ciberseguridad: comité que tendrá por objeto asesorar al Presidente de la República en materias de ciberseguridad relevantes para el funcionamiento del país, que preexistía a la ley como iniciativa del Poder Ejecutivo, compuesto por representantes de ocho subsecretarías y del aparato de inteligencia del Estado.

6.3. La coordinación regulatoria entre instituciones

La LMC dispone en el artículo 25[9] que cuando la ANCI deba dictar protocolos, estándares técnicos o instrucciones de carácter general, y éstos tengan efectos en las áreas de competencia de otra entidad sectorial, deberá previamente remitir la información relevante a dicha entidad y solicitar un informe con el propósito de prevenir posibles conflictos normativos y garantizar la coordinación, cooperación y colaboración efectivas entre ambas autoridades.

En dirección inversa, cuando una autoridad sectorial deba emitir actos administrativos de carácter general que tengan efectos en los ámbitos de competencia de la ANCI, deberá remitir a la ANCI la información pertinente y solicitar un informe con el objeto de prevenir posibles conflictos normativos y garantizar la coordinación, cooperación y colaboración.

Asimismo, se faculta a las autoridades sectoriales para emitir normativas generales, técnicas e instrucciones necesarias para fortalecer la ciberseguridad en las instituciones de su sector. Algunas de estas autoridades sectoriales son la Comisión Nacional de Energía (CNE), la Subsecretaría de Telecomunicaciones (Subtel) y la Comisión para el Mercado Financiero (CMF).

6.4. Infracciones y sanciones

La LMC otorga facultades fiscalizadoras y sancionatorias a la respectiva autoridad sectorial para sancionar y ejecutar las sanciones, las que se aplicarán conforme a la normativa sectorial sobre ciberseguridad que la autoridad haya dictado. Para esto, la normativa sectorial deberá tener efectos al menos equivalentes a los de la normativa dictada por la ANCI.

[9] Cabe destacar que esta norma es una disposición análoga, aunque adaptada a la LMC, del artículo 37 bis de la Ley N° 19.880, que establece las bases de los procedimientos administrativos que rigen los actos de los Órganos de la Administración del Estado.

De no cumplirse la equivalencia anterior, será la ANCI quien fiscalice, conozca y sancione las infracciones, estando facultada para imponer al infractor una multa a beneficio fiscal. Será también la ANCI la encargada de ejecutar las sanciones impuestas.

La multa que podrá aplicar la ANCI dependerá de la gravedad de la infracción cometida y de si el infractor se trata de OIV o de un servicio esencial sin esta calificación,[10] de acuerdo con la escala siguiente:

> Infracciones leves: se sancionarán con multa de hasta 5.000 unidades tributarias mensuales, o hasta 10.000 unidades tributarias mensuales si se trata de un OIV.
>
> Infracciones graves: se sancionarán con multa de hasta 10.000 unidades tributarias mensuales, o hasta 20.000 unidades tributarias mensuales si se trata de un OIV.
>
> Infracciones gravísimas: se sancionarán con multa de hasta 20.000 unidades tributarias mensuales, o hasta 40.000 unidades tributarias mensuales si se trata de un OIV.

7. Modificaciones legales en la LMC

7.1. Estatuto Orgánico del Ministerio de Defensa Nacional

La LMC modifica la Ley Nº 20.424 que establece estatuto orgánico del Ministerio de Defensa, al introducir una nueva letra k) al artículo 25, incorporando como función del Estado Mayor Conjunto la de "Conducir al Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional en coordinación con la Subsecretaría de Defensa".

7.2. Ley sobre delitos informáticos

Se modifica la Ley Nº 21.459 que establece normas sobre delitos informáticos ("LDI"), deroga la ley Nº 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest, introduciendo una exención al delito del artículo 2º que típica y sanciona el acceso ilícito a un sistema informático.

En efecto, no será objeto de sanción penal el que acceda a un sistema informático perteneciente a un órgano de la administración del Estado, cuyo responsable tenga domicilio en Chile, cuando lo haga cumpliendo copulativa mente con las condiciones enumeradas a continuación:

> i. Estar inscrito en el registro que al efecto lleve la ANCI;
>
> ii. Haber informado previamente a la ANCI;

[10] El tipo de infracción, conducta, las entidades obligadas y la sanción, pueden apreciarse con mayor detalle en las tablas que se muestran en el Anexo.

iii. Reportar el acceso y las vulnerabilidades de seguridad detectadas al responsable del sistema informático y a la ANCI, tan pronto se hubiere realizado;

iv. No haber realizado el acceso con ánimo de apoderarse o de usar la información contenida en el sistema informático, ni con intención fraudulenta.

v. No haber actuado más allá de lo necesario para comprobar la existencia de una vulnerabilidad, ni haber utilizado métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, exfiltración o destrucción de datos;

vi. No divulgar públicamente la información relativa a la potencial vulnerabilidad;

vii. Que se trate de un acceso a un sistema informático de los organismos de la Administración del Estado. En el resto de los casos, requerirá del consentimiento del responsable del sistema informático; y,

viii. Cumplir con las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la ANCI.

Adicionalmente, y en línea con la primera modificación, la LMC deroga el artículo 16 de la LDI, que permitía entender que quien accede, en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, a un sistema informático mediando la autorización expresa del titular del mismo, se encuentra autorizado para el acceso al respectivo sistema. Lo anterior responde a una discusión que se arrastra desde la tramitación de la LDI, pues, el ahora derogado artículo 16, al exigir la autorización expresa del titular del sistema informático, no actuaba sino como una reiteración de la tipificación realizada en el artículo 2º.

Esta situación se originó a partir del incumplimiento por parte de Chile de su declaración expresa en el instrumento de adhesión al Convenio de Budapest, donde declaró que para castigar el delito de acceso ilícito exigiría una intención criminal especifica. Sin embargo, la norma terminó por tipificar como acceso ilícito todo acceso no autorizado a sistemas informáticos (Bordachar, 2023). En este escenario,fue que el Senado propuso la introducción del artículo 16 de la LDI, que fue finalmente aprobado.[11]

[11] Al respecto, el Coordinación Nacional de Ciberseguridad, Daniel Álvarez, sostuvo durante la tramitación de la LDI que "si se pretende incorporar es una eximente de responsabilidad penal para garantizar que los investigadores de seguridad o ciberseguridad puedan desempeñar su trabajo, sin verse compelidos o amenazados con el ejercicio de la acción penal, debe hacerse en la misma norma que regula el acceso ilícito. (...). Luego, recordó que en sesiones previas se habló de la necesidad de utilizar la figura del 'deliberadamente' en este tipo de ilícitos, tal cual se hace en el artículo 1º, donde se requiere una acción positiva del titular. De otra forma, el estándar probatorio para la configuración del tipo es bastante bajo, teniendo asociado una sanción penal importante". Asimismo, destacó que "el texto propuesto para la ley marco en materia de ciberseguridad establece una cantidad de trabas y obstáculo al ejercicio de la actividad investigativa, que termina por desconocer lo que sucede en la realidad". Biblioteca del Congreso Nacional, Historia de la Ley Nº 21.459, p. 97.

En consecuencia, la LDI mantuvo la criminalización de la investigación de vulnerabilidades de los sistemas informáticos mediante pruebas de acceso sin autorización, lo que llevó a que, presumiblemente por el riesgo de incurrir en sanciones penales, los organismos públicos no efectuaran actividades de detección de vulnerabilidades y no enviaran reportes al CSIRT de Gobierno desde la entrada en vigor de la LDI.[12] De esta forma, la modificación a la LDI viene a establecer una exención que crea todo un sistema nuevo y formalizado de registro y de acceso lícito a algunos sistemas informáticos, buscando resolver una problemática que había sido largamente discutida durante la tramitación legislativa de la LDI.

[12] Así lo relató el Coordinador Nacional de Ciberseguridad, Daniel Álvarez, ante las Comisiones legislativas que examinaron el proyecto en detalle. Cfr.: Senado de Chile, "Segundo informe de las Comisiones de Defensa Nacional y de Seguridad Pública, unidas, recaído en el proyecto de ley, en primer trámite constitucional, que establece una ley marco sobre ciberseguridad e infraestructura crítica de la información, Boletín N° 14.847-06", 20 de abril de 2023.

III. La relación de la Ley Marco sobre Ciberseguridad con otros cuerpos normativos

1. La Política Nacional de Ciberseguridad 2023-2028

La preparación de una ley sobre ciberseguridad fue una de las medidas de la agenda de política pública contemplada en la Política Nacional de Ciberseguridad del año 2017. Esta medida fue materializada a través del proyecto de ley cuya tramitación culminó con la LMC. En la misma línea, la Política Nacional de Ciberseguridad del año 2023, para los años 2023 a 2028, destaca la necesidad de impulsar la tramitación, aprobación e implementación del proyecto de ley marco de ciberseguridad, para el cumplimiento de sus objetivos de que Chile cuente con una infraestructura de la información robusta y resiliente, de resguardar y promover la protección de los derechos de las personas en Internet, y de robustecer la gobernanza del país en ciberseguridad.

En ese sentido, al tratarse la LMC de una medida contemplada para la concreción de los objetivos que fueron contemplados en las políticas de ciberseguridad que se han dictado en el país, en su implementación se deberá tener especial consideración por la realización de los objetivos propuestos en tales políticas nacionales.

Por otro lado, las normas de la LMC tendrán incidencia en la creación de una futura Política Nacional de Ciberseguridad una vez agotada la política 2023-2028, pues un nuevo proceso contará con la participación de la ANCI, quien deberá asesorar al Presidente de la República en la elaboración y aprobación de la política nacional y de los planes y programas de acción para su implementación, ejecución y evaluación. Además, el Comité Interministerial sobre Ciberseguridad asesorará al Ejecutivo en el análisis y definición de la política nacional, y coordinará su implementación.

Finalmente, cabe resaltar que el Plan de Acción de la Política Nacional de Ciberseguridad 2023 se encuentra pendiente al momento de redacción del informe, siendo lógico inferir que sea la ANCI la principal entidad responsable de su implementación.

2. La reforma a la Ley de Protección de Datos Personales

Indudablemente uno de los cuerpos normativos que convergerá en mayor medida con la LMC, es la actual ley N° 19.628, sobre protección de la vida privada. En particular, atendida la discusión, en curso al momento de publicación de este informe, del proyecto de ley sobre datos personales (Boletines N°11.144-07 y 11.092-07, refundidos), que reformula toda la protección de datos personales en Chile.

La LMC tiene especial consideración por la protección de los datos personales. Lo anterior se aprecia en distintas normas:

i. El principio de seguridad y privacidad por defecto y desde el diseño busca precisamente la seguridad y privacidad de los datos personales que se procesan.[13]

ii. Se establece como un deber de los OIV informar a potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieren comprometer gravemente su información o redes y sistemas informáticos, en especial si involucran datos personales y no existe otra disposición que requiera su notificación. [14]

iii. En el marco de la atribución de la ANCI para requerir a los organismos públicos y privados acceso a la información necesaria para prevenir incidentes o gestionar uno ya ocurrido, se establece la obligación de las entidades de anonimizar datos personales siempre que sea posible. Además, se establece que tales datos solo podrán tratarse en estricto cumplimiento de la Ley Nº 19.628 y del principio de finalidad del tratamiento de datos personales.[15]

iv. Los incidentes que afecten a sistemas informáticos que contienen datos personales, se consideran incidentes de efecto significativo. Además, en los reportes que emitan al respecto, debe omitirse todo dato personal.[16]

v. Finalmente, se establece que la ANCI debe procurar el respeto de los derechos fundamentales de las personas y, en particular, procurar respetar y resguardar el derecho a la vida privada y a la protección de los datos personales.[17]

La Ley Nº 19.628, que ante todo regula el tratamiento de datos personales, continuará vigente en sus términos actuales al menos durante los dos años siguientes a partir de que se convierta en ley el proyecto de ley de datos personales que la modifica sustancialmente, y aprobado durante 2024.

Dicho proyecto de ley contempla la introducción de deberes y normas que reforzarán los deberes relativos a seguridad de sistemas informáticos que contengan datos personales. Además, el proyecto crea una nueva autoridad de control de datos personales, la Agencia de Protección de Datos Personales, y el deber de reportar a esta las vulneraciones a las medidas de seguridad. Este deber de reportar se suma al que contempla la LMC para los mismos incidentes. Asimismo, dado que el proyecto de ley otorga facultades fiscalizadoras y sancionadoras a la Agencia de Protección de Datos Personales, se deberá cuidar que el ámbito de cada agencia quede suficientemente delimitado a efectos de que no se generen dudas o contiendas respecto a la competencia sobre un incidente que vulnere datos personales contenidos en sistemas informáticos.

13 LMC, artículo 3º, Nº8.

14 LMC, artículo 8º, letra g).

15 LMC, artículo 11, letra j).

16 LMC, artículo 27.

17 LMC, artículo 35.

Igualmente, es posible que ciertos OIV sean a la vez responsables de tratamiento de datos personales, o terceros mandatarios o encargados de tratamiento de tales datos. Cuando este sea el caso, estas entidades serán sujetos obligados simultáneamente por ambos cuerpos legales. En ese sentido, el principio de coordinación y la coordinación regulatoria serán clave para conjugar las funciones y facultades de ambas agencias.

3. La Ley sobre delitos informáticos

Uno de los aspectos centrales que fue tenido en cuenta durante la discusión legislativa de la LMC es la debida armonía que debía guardar la LMC tanto con el proyecto de ley de datos personales, como con la Ley N° 21.459 sobre delitos informáticos. Al respecto, durante la tramitación de la ley se expresó que la ciberseguridad es un sistema que se compone de estos tres estatutos legales: la LMC, el proyecto de ley de datos personales, y la ley de delitos informáticos.[18]

La necesidad de armonizar la LMC con la ley de delitos informáticos impulsó al legislador a establecer una nueva exención de responsabilidad aplicable al delito informático de acceso ilícito regulado en el artículo 2° de la ley, permitiendo lo que se conoce como "hacking ético", bajo ciertas condiciones. Lo anterior, con el propósito de mejorar la calidad de los sistemas y propender a mejorar su seguridad.

Sin embargo, conviene realizar ciertas apreciaciones respecto a la norma aprobada. La norma estableció como una de las condiciones para la aplicación de la exención de responsabilidad penal "[h]aber dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la Agencia". Con este requisito, la modificación a la LDI solo podrá ser efectiva una vez que la ANCI dicte las normas que contengan las "demás condiciones" para que proceda la excepción en comento. Esta condición abierta, que la LMC deja a determinación de la ANCI, no es problemática únicamente por el hecho de que su aplicación efectiva se podría ver significativamente postergada, sino que, además, puede conllevar dificultades desde la órbita del principio de tipicidad que envuelve al derecho penal, pues cabe preguntarse hasta qué punto una exención a un tipo penal se encuentra determinada por una norma de rango infralegal, en este caso, dictada por la ANCI.

Lo anterior, en conjunto con el resto de las condiciones necesarias para el desarrollo del llamado "hacking ético", abre la interrogante sobre qué tan efectiva llegará a ser

[18] Coordinador Nacional de Ciberseguridad, "Informe de la Comisión de Seguridad Pública del Senado recaído en el proyecto de ley, en primer trámite constitucional, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información", 12 de octubre de 2022, p. 13.

la norma en la práctica y si permitirá resolver el problema de falta de reportes de vulnerabilidades en los sistemas públicos que se generó con la promulgación de la ley de delitos informáticos.[19]

4. La Ley Nº 21.180 sobre transformación digital del estado

Por su parte, la ciberseguridad es uno de los ejes relevantes de la reforma introducida por la Ley Nº 21.180, de transformación digital del estado, a la Ley Nº 19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.

Al respecto, se dispone que las plataformas electrónicas utilizadas por los órganos de la Administración del Estado deben cumplir con los estándares de ciberseguridad fijados en el reglamento (artículo 19). De este modo, fija un deber de cumplimiento de estándares favorable a la seguridad de los sistemas.

A mayor abundamiento, el Reglamento de la Ley de transformación digital del Estado establece estándares de ciberseguridad, obligando a los órganos de la Administración a desarrollar una política de ciberseguridad (artículo 46) que contenga, a lo menos, los elementos enumerados a continuación:

> i. Uso adecuado y eficaz de la criptografía sobre la información para el almacenamiento, transferencia y acceso del expediente y de la información en ellos contenida.
>
> ii. Mitigación de los riesgos de captura o suplantación de información, por personas o sistemas no autorizados, siguiendo las directrices de la Norma Técnica de Interoperabilidad.
>
> iii. Control de acceso a las plataformas, en la generación, almacenamiento y caducidad de perfiles de acceso.

La referida política debe basarse en la norma técnica de ciberseguridad y seguridad de la información a la que hace alusión el artículo 57 del Reglamento, la que deberá determinar los estándares y normas técnicas que deberán cumplir los órganos de la Administración del Estado para resguardar la confidencialidad, integridad y disponibilidad de la información, así como proteger la infraestructura informática.

---

[19] *Ibid.* Al respecto, en el segundo informe de las Comisiones de Defensa Nacional y de Seguridad Pública, unidas, del Senado, de 20 de abril de 2023, se explicó la enmienda al artículo 2º de la Ley sobre delitos informáticos fue anteriormente discutida durante la tramitación de dicha ley. En esa oportunidad, se debatió la posibilidad de proteger legalmente al investigador en seguridad informática que descubre una vulnerabilidad y sigue un procedimiento para notificar al afectado a fin de resolverla. Sin embargo, con su entrada en vigor, el CSIRT de Gobierno dejó de recibir reportes relativos a las debilidades presentes en los sistemas públicos, en atención a que ello podría conllevar sanciones penales. Lo anterior, llevó a proponer un resguardo legal al hacking ético durante la tramitación del proyecto de LMC.

Con la entrada en vigencia de la LMC, el cumplimiento de las obligaciones impuestas por esta normativa sectorial pasará a ser uno de los deberes generales que establece la LMC para las entidades reguladas. Además, la elaboración de las políticas y acciones relativas a ciberseguridad que implementen los organismos de la Administración del Estado, contará con la colaboración o asesoría del CSIRT Nacional, y deberán tener efectos a lo menos equivalentes a las obligaciones previstas en los protocolos, normas o instrucciones de la ANCI, para que prevalezcan por sobre la regulación dictada por esta.

Para lo anterior, la ANCI y la autoridad sectorial deberán dictar una norma conjunta de carácter general, que establezca criterios para la evaluación de equivalencia de los efectos de las regulaciones, con lo que lo que el principio de coordinación y la coordinación regulatoria vuelven a cobrar relevancia.

5. La Política Nacional de Inteligencia Artificial

La Política Nacional de Inteligencia Artificial del 2021 reconoce a la Inteligencia Artificial como una herramienta para la mantención de un ciberespacio libre, abierto, seguro y resiliente, cumpliendo con los objetivos de la Política Nacional de Ciberseguridad.

En esa línea, uno de los objetivos planteados fue posicionar la IA como un componente relevante de la ciberseguridad y ciberdefensa, promoviendo sistemas tecnológicos seguros, para lo que se incorporaría la IA en las estrategias de ciberseguridad y en los proyectos de ley asociados. No obstante, y si bien la Política Nacional de Inteligencia Artificial y la IA fueron contempladas en la Política Nacional de Ciberseguridad dictada en 2023, la LMC no hace referencias a la IA.

6. Proyectos de ley relacionados

Una serie de proyectos de ley, en discusión activa en el Congreso chileno al momento de finalización del presente informe, podrían todavía afectar el funcionamiento del esquema creado por la LMC. Esto incluye:

1. Proyecto de ley sobre Inteligencia Artificial (Boletín Nº 15.869-19)
El proyecto de ley que regula los sistemas de inteligencia artificial, la robótica y las tecnologías conexas en sus distintos ámbitos de aplicación, ingresado a la Cámara de Diputados y Diputadas mediante moción en abril de 2023, contempla para la autorización de un sistema de IA calificado de alto riesgo, entre otros requisitos,

que demuestre cumplir con un nivel adecuado de ciberseguridad. En ese sentido, la implementación de la LMC y los estándares y normas que desarrolle la ANCI, podrían ser relevantes para definir cuál será el nivel adecuado de ciberseguridad en esta materia.[20]

2. Proyecto de ley sobre Infraestructura Crítica (Boletín Nº 16.143-02)

A partir del año 2019 ingresaron al Congreso Nacional varios proyectos de ley que buscaban reformar la Constitución Política de la República para permitir el empleo de las Fuerzas Armadas para el resguardo de infraestructura crítica del país. Entre ellos, se encontraba el Boletín Nº 15219-07, refundido con el Boletín Nº 13085-07, que se convirtió en la ley Nº 21.542, publicada en el Diario Oficial el 3 de febrero de 2023.

Dicha reforma consagró en el artículo 32 de la Constitución Política de la República un nuevo numeral 21, que faculta al Presidente de la República para disponer que las Fuerzas Armadas se hagan cargo de la protección de la infraestructura crítica del país cuando exista peligro grave o inminente. Además, se estableció en la Constitución una disposición quincuagésima tercera transitoria, por la que se mandató al Presidente de la República a enviar en un plazo de seis meses desde publicada la reforma constitucional, un mensaje con un proyecto de ley con el objetivo de regular las materias que señala el nuevo numeral 21 del artículo 32 de la Constitución.

El proyecto de ley para la protección de la infraestructura crítica del país, ingresado por el Presidente de la República al Senado en agosto de 2023, busca dar cumplimiento a lo mandatado por la reforma constitucional antedicha, y tiene por objeto establecer una regulación en favor del resguardo de los operadores públicos y privados de infraestructura crítica.

La propuesta excluye las redes y sistemas informáticos que son regulados por la LMC, al definir la infraestructura crítica como "el conjunto de instalaciones, sistemas físicos o servicios esenciales y de utilidad pública". Así, de convertirse en ley, esta protegerá la infraestructura crítica en su faceta "física" excluyendo los incidentes que se produzcan en la faceta "virtual" de una institución.

Más allá de la distinción que el legislador busca instaurar al respecto, ambos cuerpos legales podrían llegar a ser aplicables ante los mismos ataques. En efecto, varias de las categorías de servicios esenciales que define la LMC coinciden con las industrias que se incluyen dentro de la infraestructura de ley de este proyecto. Lo anterior es del todo lógico, pues un ciberataque a las redes o sistemas

[20] *N. del E.:* En mayo de 2024, el Ejecutivo presentó un nuevo proyecto de ley sobre la misma materia, Boletín Nº 16821-19, que eventualmente sería refundido con el Boletín Nº 15869-19. El nuevo proyecto incluye obligaciones generales de seguridad, como también obligaciones específicas de "un nivel adecuado de precisión, solidez, seguridad y ciberseguridad" para los sistemas de IA de alto riesgo.

informáticos de un servicio esencial, que constituye al mismo tiempo un operador de infraestructura crítica, podría conllevar la afectación de la infraestructura "física" de la respectiva entidad.

3. Anuncio de proyecto de ley sobre gobernanza de datos

El 22 de enero de 2024 tuvo lugar la primera sesión de la mesa de trabajo para la elaboración de un proyecto de ley sobre gobernanza de datos.

Los objetivos anunciados son los siguientes:

i. Armonizar la dispersión regulatoria en materia de interoperabilidad e intercambio de datos.
ii. Habilitar el intercambio de datos más allá de la Administración del Estado.
iii. Dotar de un marco común a las nuevas instituciones relacionadas con datos: Agencia de Ciberseguridad, Agencia de Protección de Datos y Secretaría de Gobierno Digital.
iv. Agilizar la implementación de la Ley de Transformación Digital del Estado.

Esta instancia representa una labor necesaria para entregar armonía y coordinar la gobernanza que se instaurará con la implementación de los estatutos legales de ciberseguridad y de protección de datos personales.

IV. La implementación de la LMC y sus desafíos

1. La puesta en marcha de la LMC

Con la fecha de publicación de la LMC en el Diario Oficial (el 8 de abril de 2024), comenzarán a correr los plazos que la ley establece para su vigencia y la dictación de la normativa complementaria. Desde esa fecha, el Presidente de la República contará con un año para dictar, a través del Ministerio del Interior y Seguridad Pública, uno o más decretos con fuerza de ley que establecerán la regulación de diversas materias. Entre estas materias, se encuentran:

i. La determinación de la fecha para la iniciación de actividades de la ANCI, la cual podrá contemplar un período para su implementación y uno a contar del cual entrará en operaciones.

ii. La determinación de un periodo para la vigencia de las normas establecidas por la presente ley el cual no podrá ser inferior a seis meses desde su publicación.

El Ministerio del Interior y Seguridad Pública contará con un plazo de 180 días desde la publicación de la LMC en el Diario Oficial para expedir los reglamentos a los que se refiere la ley. Dentro de las materias que deberán ser reguladas por estos reglamentos se encuentran las siguientes:

i. Determinar los aspectos del procedimiento de calificación de operadores de importancia vital no contemplados en la LMC. Entre ellos, la forma en que se efectuará la consulta pública de la nómina preliminar elaborada por la ANCI y la forma de individualizar en la nómina final a las instituciones calificadas como operadores de importancia vital (artículo 6).

ii. Determinar ciertos aspectos de los deberes que la LMC impone a los operadores de importancia vital, como la forma en que éstos deberán mantener registro de las acciones ejecutadas que compongan el sistema de gestión de seguridad de la información (artículo 8º, letra b)); y, la forma en que realizarán operaciones de revisión, ejercicios, simulacros y análisis de redes y sistemas para detectar acciones o programas que comprometan la ciberseguridad y comunicar la información al CSIRT Nacional (artículo 8º, letra d)).

iii. El contenido de las diversas clases de reporte a las que se refiere el artículo 9º, que establece el deber de reportar los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos.

iv. La forma en que la ANCI, en el marco de sus atribuciones, efectuará el requerimiento para acceder a redes y sistemas informáticos en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible (artículo 11, letra k)); y,

los casos y las condiciones para otorgar y revocar las acreditaciones a los centros de certificación (artículo 11, letra u).

v. Establecer la estructura interna de la ANCI (artículo 17).

vi. Determinar las normas para el correcto funcionamiento del Consejo Multisectorial sobre Ciberseguridad (artículo 21).

vii. Regular el funcionamiento de la Red de Conectividad Segura del Estado y las obligaciones especiales de los organismos de la Administración del Estado.

viii. El procedimiento de notificación de incidentes de ciberseguridad, la forma, las condiciones de anonimato, la taxonomía del informe y la periodicidad (artículo 27).

ix. La forma de las notificaciones por correo electrónico del procedimiento administrativo sancionador (artículo 42, letra a).

x. Las normas de funcionamiento del Comité Interministerial sobre Ciberseguridad (artículo 52).

Al respecto, el Coordinador Nacional de Ciberseguridad, explicó que la implementación de la LMC depende de una serie de hitos que contempla la dictación de reglamentos que definirán "la estructura del servicio de la ANCI", y "los recursos humanos y financieros", lo que debiese cumplirse en septiembre de 2024. Asimismo, es relevante la dictación de los decretos con fuerza de ley relativos a la dotación y al presupuesto. Finalmente, el Coordinador explicó que los servicios regulados "debieran contar con todo este año que no van a estar obligados para que empiecen a tomar medidas organizativas necesarias".[21] A la fecha de cierre del presente documento, la normativa complementaria no ha sido dictada.

2. Desafíos y puntos pendientes

La LMC representa un avance significativo en cuanto a normativa, estándares, gestión de riesgos, institucionalidad y gobernanza en materia de seguridad de redes y sistemas informáticos. Sin embargo, su implementación llevará a las entidades públicas y privadas reguladas por esta norma a tener que realizar grandes esfuerzos por adaptarse a la nueva legislación, lo que sin duda supondrá un desafío tanto a nivel económico, como de logística, recursos humanos, capacidades y conocimiento.

[21] Diario Financiero, "Senado presentó los ejes de la hoja de ruta del Foro Nacional de Ciberseguridad", DF LAB, 2 de abril de 2024, disponible en: https://t.ly/Z0RgD.

En efecto, las empresas que presten servicios esenciales y los órganos de la Administración del Estado deberán solventar los altos costos que puede conllevar adoptar las medidas y estándares de ciberseguridad que exige la LMC. Asimismo, deberán afrontar la falta de conocimiento y la carencia de especialistas que existe en el país en materias de ciberseguridad.

A mayor abundamiento, aún es necesario que los reglamentos de implementación y la labor que desarrolle la ANCI logren aclarar diversos puntos de la LMC que son importantes para la correcta y oportuna adecuación de las empresas que realizan actividades esenciales.

En esa línea, a modo de ejemplo, no existe suficiente precisión sobre la definición de servicios esenciales. La enunciación de actividades que se realiza en el artículo 4° puede resultar confusa por sí misma, al contemplar como servicios esenciales los prestados por empresas que difícilmente podrían ser consideradas tales a la luz de su relevancia económica o para el funcionamiento de la sociedad, o por no representar su afectación un riesgo de que se cause un grave daño a la población o al abastecimiento. Por ejemplo, basta con preguntarnos si hay casos en que podría calificar como un servicio esencial cualquier empresa que preste servicios digitales sin importar la naturaleza de dicho servicio.

Asimismo, fuera de las actividades que la LMC califica como servicios esenciales, existe también ambigüedad sobre los criterios que se utilizarán para calificar otros servicios como esenciales. Esta falta de precisión se extiende a la calificación de OIV. En ese sentido, la labor de la ANCI en la definición de estos criterios deberá realizarse con el mayor cuidado posible, sobre todo si consideramos que los prestadores que califiquen como OIV tienen obligaciones específicas cuya infracción puede acarrear multas cuantiosas que llegan hasta las 40.000 unidades tributarias mensuales (sobre los dos millones y medio de dólares de los EE.UU.).

Por otro lado, las preocupaciones relativas a la incertidumbre para las empresas privadas que quedarán bajo el ámbito de aplicación de la LMC, es mayor tratándose de pequeñas y medianas empresas que pudieran ser obligadas, y para quienes los costos de adecuación serán mucho más significativos. Al respecto, la LMC se limita a establecer que la calidad de pequeña y mediana empresa será “especialmente” considerada por la ANCI para la calificación de operadores de importancia vital y para establecer medidas de seguridad diferenciadas, con expresa remisión a la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño..

Frente a lo señalado, el principio de coordinación y la coordinación regulatoria representan la mejor herramienta para facilitar la adaptación a la nueva regulación. El rol y trabajo proactivo de la ANCI será crucial en este sentido.

Por último, cabe destacar que la necesidad de contar con una normativa de protección de datos personales actualizada y consistente con la realidad actual, es más apremiante que nunca tras la dictación y eminente implementación de la LMC. Los ciberataques e incidentes que implican la afectación de datos personales requieren la actuación conjunta y coordinada de la autoridad de datos y de la autoridad de ciberseguridad. En definitiva, un sistema de ciberseguridad, cuando implica el resguardo de datos personales, no puede funcionar adecuadamente sin una legislación robusta en materia de datos personales que se ajuste a los estándares internacionales y a la realidad del país.

V. Consideraciones finales y recomendaciones

La nueva Ley Marco de Ciberseguridad representa un gran paso para el desarrollo de la ciberseguridad en Chile y para la protección de los organismos públicos, las empresas y los derechos de las personas en el ciberespacio. Pone a Chile como ejemplo de discusión legislativa en materias avanzadas de manera eficiente e inclusiva de distintas visiones sobre la materia, en un rol pionero en la región.

Sin embargo, la concreción de los objetivos de la nueva regulación dependerá en gran medida de lo que ocurra durante su implementación. Las próximas etapas serán fundamentales para dar vida al nuevo marco regulatorio de forma exitosa. La dictación de los reglamentos, su entrada en vigencia y la instalación de la Agencia Nacional de Ciberseguridad y de las demás entidades creadas, serán esenciales para la clarificación de ciertos aspectos de la ley y para que los sujetos regulados puedan adaptarse a los nuevos estándares y obligaciones.

La inserción de la LMC en el contexto regulatorio nacional es un proceso complejo, pues deberá integrarse en un entramado legal existente, complementando y fortaleciendo las disposiciones vigentes relacionadas con la seguridad de los sistemas informáticos.

Lo anterior, va más allá de la ejecución de los incontables aspectos técnicos de la LMC, sino que, su implementación depende, por sobre todo, de aspectos sistémicos que conllevarán grandes esfuerzos financieros, de coordinación y adecuación por parte de las autoridades y sujetos regulados, y un cambio cultural en torno al resguardo de la ciberseguridad.

Por último, cabe resaltar que, tras la dictación de la LMC, resulta urgente contar con una normativa de protección de datos personales actualizada, pues las ciberamenazas y ciberataques que afectan datos personales requieren una legislación robusta en esta materia, además de la actuación conjunta y coordinada de las autoridades que se crearan en virtud de ambas normativas.

Por estas razones, es recomendable para la implementación de la LMC que el Estado de Chile considere:

i. **Transparencia en el proceso de implementación de la LMC.** El proceso de implementación de la LMC y la instalación de la ANCI y de las demás entidades reguladas, se debe desarrollar con transparencia, garantizando la confianza el proceso y la entrega proactiva de la información y del apoyo necesarios para que los organismos y empresas reguladas puedan adecuarse satisfactoriamente a la nueva regulación.

ii. Participación en el proceso de implementación de la LMC. El proceso de implementación de la LMC y la instalación de la ANCI y de las demás entidades reguladas, debe contar con la participación de los sujetos regulados y de otros interesados, quienes podrán aportar su experiencia y conocimiento para una implementación exitosa de la LMC. Es esencial que dicha participación sea inclusiva, comprendiendo a distintos sectores, instando a participar a organismos y empresas reguladas de las más diversas áreas, así como a expertos y organizaciones de la sociedad civil, de forma de garantizar que la implementación de la LMC refleje las preocupaciones de todos los sectores que se verán afectados por la nueva regulación. Esto puede hacerse a través de consultas públicas, mesas de trabajo, la institucionalidad de los Consejos de Sociedad Civil establecidos por la Ley N° 20.500 u otros mecanismos.

iii. Protección de los derechos de las personas. Las medidas que se adopten para la implementación de la LMC, así como las medidas adoptadas por los sujetos regulados, deben considerar la protección de los derechos de las personas y la protección preferente de ciertas dimensiones transversales que han sido definidas por la Política Nacional de Ciberseguridad 2023-2028. Así, se debe considerar la equidad de género, la infancia, a los adultos mayores y al medio ambiente, como dimensiones y/o grupos humanos que deben ser especialmente considerados en el desarrollo y fortalecimiento la ciberseguridad en el país.

iv. Diversidad, inclusión y equidad en la composición del Consejo Multisectorial sobre Ciberseguridad. La creación del Consejo Multisectorial sobre Ciberseguridad en la ANCI, con carácter consultivo, es uno de los elementos de participación más llamativos en el contexto de la gobernanza de la ciberseguridad. Su composición es una materia altamente sensible, debido a la posibilidad que abre para la incorporación de diversos intereses a la implementación de medidas de ciberseguridad. Por esta razón, tanto su composición como su funcionamiento deben considerar especialmente la inclusión de perspectivas de personas no solamente de distintos sectores productivos, sino de distintos perfiles sexogenéricos, etarios, educativos, geográficos, y representantes de los intereses de grupos históricamente marginalizados o en situación de vulnerabilidad.

v. Especial protección de los derechos de mujeres y niñas. Es crucial que durante este proceso se considere de forma preferente a las mujeres y niñas, incluyendo medidas específicas para promover su participación activa y la protección de sus derechos. Para ello, se debe considerar que las mujeres y niñas suelen ser las principales víctimas de la violencia presente en el ciberespacio, como también la baja participación en puestos laborales y espacios de decisión relacionados con la ciberseguridad. Asimismo, se insta a poner especial atención a la protección de la privacidad y los datos personales de mujeres y niñas, con el objetivo de que el ejercicio de sus derechos fundamentales se encuentre garantizado en el entorno digital.

Bibliografía

– Bordachar, Michelle (2023). "La exención de responsabilidad por autorización o investigación académica". En: Samuel Malamud y Guillermo Chahuán (Coords.). Delitos Informáticos, Análisis Dogmático y Comentarios a la Ley N° 21.459. pp. 339-368.

– Urzúa, Jaime (2022). "Los ciberataques masivos más importantes de 2022", Diario Constitucional, 12 de octubre de 2022, disponible en: https://www.diarioconstitucional.cl/estudios-juridicos/los-ciberataques-masivos-mas-importantes-de-2022-por-jaime-urzua/

– Biblioteca del Congreso Nacional, Historia de la Ley N° 21.459.

– Gobierno de Chile, Política Nacional de Ciberseguridad 2017-2022.

– Gobierno de Chile, Política Nacional de Ciberseguridad 2023-2028.

– Gobierno de Chile, Política Nacional de Inteligencia Artificial, 2021.

– Ley N° 19.628 sobre protección de la vida privada

– Ley N° 21.459 que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.

– Ley N° 21.180 sobre transformación digital del estado.

– Ley N° 21.663, Ley Marco de Ciberseguridad

– Proyecto de ley Boletín N° 11.144-07, refundido con el Boletín N° 11.092-07, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.

– Proyecto de ley Boletín N° 15.869-19, que regula los sistemas de inteligencia artificial, la robótica y las tecnologías conexas, en sus distintos ámbitos de aplicación.

– Proyecto de ley Boletín N° 16.143-02, para la protección de la infraestructura crítica del país.

– Tribunal Constitucional, Sentencia Rol N° 15.043-23, "Control de constitucionalidad del proyecto de ley que establece una ley marco sobre ciberseguridad e infraestructura crítica de la información, correspondiente al boletín N° 14.847-06", 19 de marzo de 2024.

Anexo: Infracciones, conductas, entidades obligadas y sanciones que contempla la LMC

Infracciones leves		
Conducta	Obligado	Sanción
Entregar fuera de plazo la información que se le requiera cuando ella no fuere necesaria para la gestión de un incidente de ciberseguridad.	Todos	Multa de hasta 5.000 U.T.M., o hasta 10.000 U.T.M si se trata de un operador de importancia vital.
Incumplir las instrucciones generales o particulares impartidas por la ANCI en los casos que no esté sancionado como infracción grave o gravísima.	Todos	
Cualquier infracción a las obligaciones que la ley establece y que no tenga señalada una sanción especial.	Todos	
No mantener el registro de las acciones de seguridad que señala la letra b) del articulo 8°.	OIV	Multa de hasta 10.000 U.T.M
No comunicar al CSIRT Nacional la realización continua de operaciones de revisión, ejercicios y demás acciones que señala la letra d) del artículo 8°	OIV	
No contar con programas de capacitación, formación y educación continua para los trabajadores, según dispone la letra h) del artículo 8°.	OIV	
No designar un delegado de ciberseguridad, según dispone la letra i) del artículo 8°.	OIV	
No dar cumplimiento a la instrucción particular de la ANCI en orden a certificar los planes de continuidad operacional del párrafo segundo de la letra c) del artículo 8°.	OIV	
No contar con las certificaciones que exija la ley, de acuerdo con la letra f) del artículo 8°.	OIV	

Infracciones graves		
Conducta	Obligado	Sanción
No haber implementado los protocolos y estándares establecidos por la Agencia para prevenir, reportar y resolver incidentes de ciberseguridad.	Todos	Multa de hasta 10.000 U.T.M., o hasta 20.000 U.T.M. si se trata de un operador de importancia vital.
No haber implementado los estándares particulares de ciberseguridad.	Todos	
Entregar fuera de plazo la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de ciberseguridad.	Todos	
Entregar a la ANCI información manifiestamente falsa o errónea.	Todos	
Incumplir la obligación de reportar establecida en el artículo 9º.	Todos	
Negarse injustificadamente a cumplir una instrucción de la ANCI o entorpecer deliberadamente el ejercicio de las atribuciones de la ANCI durante la gestión de un incidente de ciberseguridad, siempre que la atribución no cuente con una sanción especial.	Todos	
La reincidencia en una misma infracción leve dentro de un año.	Todos	
No haber implementado el sistema de gestión de seguridad de la información continuo al que se refiere la letra a) del artículo 8º.	OIV	Multa de hasta 20.000 U.T.M
No haber elaborado o implementado los planes de continuidad operacional y ciberseguridad a los que se refiere la letra c) del artículo 8º.	OIV	

Infracciones graves		
Conducta	Obligado	Sanción
No informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, en los casos que señala la letra g) del artículo 8°.	OIV	Multa de hasta 20.000 U.T.M
No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e) del artículo 8°.	OIV	
La reincidencia en una misma infracción leve dentro del período de un año.	OIV	

Infracciones gravísimas		
Conducta	Obligado	Sanción
Entregar a la ANCI información manifiestamente falsa o errónea, cuando ella sea necesaria para la gestión de un incidente de ciberseguridad.	Todos	Multa de hasta 20.000 U.T.M., o hasta 40.000 U.T.M. si se trata de un operador de importancia vital.
Incumplir las instrucciones generales o particulares impartidas por la ANCI durante la gestión de un incidente de impacto significativo.	Todos	
No entregar la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de impacto significativo.	Todos	
La reincidencia en una infracción grave dentro de un año.	Todos	
No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e) del artículo 8°, cuando éste posea un impacto significativo.	OIV	Multa de hasta 40.000 U.T.M.
La reincidencia en una misma infracción grave dentro del período de un año.	OIV	


DERECHOS
DIGITALES
América Latina