Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información

I. Introducción

a) Promulgación

Con fecha de hoy, 26 de marzo, el Presidente de la República promulgó la "*Ley Marco sobre Ciberseguridad e Infraestructura Crítica*" ("LMC").

b) Objeto de la LMC

La LMC tiene por principal objeto establecer (artículo 1):

- 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;
- los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad;
- las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones que presten servicios calificados como esenciales y aquellas calificadas como operadores de importancia vital (artículos 4°, 5° y 6°),
- los mecanismos de control, supervisión y de responsabilidad ante infracciones.

Para alcanzar los objetivos señalados, se deberá observar los siguientes principios:

(i) principio de control de daños: frente a un incidente, siempre se deberá actuar coordinada y diligentemente, y adoptar las medidas necesarias para evitar su escalada y su posible propagación a otros sistemas informáticos.

(ii) principio de cooperación con la autoridad: para resolver los incidentes, se deberá prestar la cooperación debida con la autoridad competente y, de ser necesario, cooperar entre diversos sectores, considerando la interconexión y dependencia de los sistemas.

(iii) principio de coordinación: la Agencia y las autoridades gubernamentales deberán cumplir sus cometidos coordinadamente, propender a la unidad de acción y evitar la duplicación o interferencia de funciones.

(iv) principio de seguridad en el ciberespacio: es deber del Estado resguardar la seguridad del ciberespacio, velando para que todas las personas puedan participar de un ciberespacio seguro, otorgando especial protección a las redes y sistemas informáticos que contengan información de aquellos grupos de personas que suelen ser en mayor medida objeto de ciberataques.

(v) principio de respuesta responsable: la aplicación de medidas para responder a incidentes en ningún caso podrá significar la realización o el apoyo a operaciones ofensivas.

(vi) principio de seguridad informática: toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el cifrado.

(vii) principio de racionalidad: las medidas para la gestión de incidentes, las obligaciones de ciberseguridad y el ejercicio de las facultades de la Agencia, deberán ser necesarias y proporcionadas al grado de exposición a los riesgos, y al eventual impacto social y económico.

(viii) principio de 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.

II. Ámbito de aplicación de la LMC

La LMC aplicará a aquellas instituciones que presten servicios calificados como *esenciales* según lo establecido en su artículo 4, y también a aquellas que sean calificadas como *operadores de importancia vital*, de conformidad con lo dispuesto en los artículos 5° y 6° de la misma ley.

a) Promulgación

Con fecha de hoy, 26 de marzo, el Presidente de la República promulgó la "*Ley Marco sobre Ciberseguridad e Infraestructura Crítica*" ("LMC").

Servicios esenciales: La LMC señala en su art. 4° que son servicios esenciales:

(i) aquellos provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional;

(ii) los prestados bajo concesión de servicio público, y

(iii) los proveídos por instituciones privadas que realicen las siguientes actividades:

· generación, transmisión o distribución eléctrica;

· 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 por terceros;

· transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva;

· banca, servicios financieros y medios de pago;

· administración de prestaciones de seguridad social;

· servicios postales y de mensajería;

· prestación institucional de salud por entidades tales como hospitales, clínicas, consultorios y centros médicos, y

· la producción y/o investigación de productos farmacéuticos.

(iv) aquellos servicios que la Agencia califique como esenciales mediante resolución fundada del Director Nacional 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.

III. Obligaciones de ciberseguridad

Las instituciones obligadas por la LMC deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad, las cuales podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso, debiendo cumplir con los protocolos y estándares establecidos por la Agencia, así como los estándares particulares dictados de conformidad a la regulación sectorial respectiva.

Para ello se establecen deberes específicos de los *operadores vitales* (artículo 8°) y se establece un listado de casos en que las instituciones públicas y privadas tendrán la obligación de reportar al Equipo de Respuesta a Incidentes de Ciberseguridad Informática Nacional ("CSIRT Nacional") los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos (artículo 9°), disponiendo diversas clases de reportes cuyo contenido será regulado por un reglamento.

IV. Creación de la Agencia Nacional de Ciberseguridad y CSIRT Nacional

Se crea la Agencia Nacional de Ciberseguridad como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, de carácter técnico y especializado, cuyo objeto será (artículo 10):

1. Asesorar al Presidente de la República en materias propias de ciberseguridad,
2. Colaborar en la protección de los intereses nacionales en el ciberespacio,
3. Coordinar el actuar de las instituciones con competencia en materia de ciberseguridad,
4. Velar por la protección, promoción y respeto del derecho a la seguridad informática, y
5. Coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

A continuación, la LMC establece las atribuciones para el cumplimiento de dicho objeto (artículo 11) dentro de las cuales, destacada la facultad de requerir, mediante instrucción de su Director/a, en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible, el acceso a redes y sistemas informáticos, sin perjuicio del derecho a oponerse de las instituciones privadas requeridas.

Asimismo, se crea dentro de la Agencia, el CSIRT Nacional, el que tendrá, entre otras, la función de responder ante ciberataques o incidentes de ciberseguridad de efecto significativo.

V. Infracciones y sanciones a la ley

Autoridad Competente.

La LMC señala que la autoridad sectorial será competente para fiscalizar, conocer y sancionar las infracciones, así como ejecutar las sanciones a la normativa sobre ciberseguridad que hubiere dictado y cuyos efectos sean al menos equivalentes al de la normativa dictada por la Agencia. Para este efecto, las sanciones y procedimientos sancionatorios serán los que correspondan a la autoridad sectorial de conformidad a su normativa.

Sin embargo, fuera de dichos casos, corresponderá a la Agencia fiscalizar, conocer y sancionar las infracciones, así como ejecutar las sanciones a la presente ley, sin perjuicio de la facultad de los organismos de la Administración del Estado de poner en conocimiento del organismo competente las infracciones a la norma de que tomaren conocimiento.

Infracciones.

Para ello, las infracciones se categorizan en leves, graves y gravísimas (Art. 38), estableciendo un régimen especial de infracción al art. 8º de la LMC por los operadores de importancia vital (Art. 39).

Sanciones.

La LMC establece multas de acuerdo a la gravedad de la infracción: hasta 5.000 UTM para infracciones leves, hasta 10.000 UTM para infracciones graves, y hasta 20.000 UTM para infracciones gravísimas. Estos montos se duplican en el caso de *operadores de importancia vital*. La fijación de la multa toma en cuenta factores como las medidas de seguridad implementadas, la probabilidad de ocurrencia del incidente, la gravedad de los efectos de los ataques, y la capacidad económica del infractor.

Procedimiento.

La LMC establece un Procedimiento Administrativo Sancionador Simplificado para aquellos casos en que las infracciones imputadas sean calificadas como leves, en cuyo caso la Agencia estará facultada para proponer de manera inmediata la sanción a aplicar, la cual quedará firme si el presunto infractor opta por allanarse a los cargos formulados en su contra (Art. 41).

Luego, se establece el Procedimiento Administrativo Sancionador general (Art. 42), el cual se regirá en el procedimiento contenido en la Ley N° 19.880 (que establece las bases de los procedimientos administrativos que rigen los actos de los organismos de las Administracion del Estado), señalando disposiciones particulares. Corresponderá al subdirector de la Agencia resolver los procesos sancionatorios, procediendo en contra de su resolución los recursos que establezca la ley N° 19.880.

Finalmente, la LMC establece un Procedimiento de Reclamación Judicial (Art. 46), en virtud del cual las personas que estimen que un acto administrativo que paraliza el procedimiento, o una resolución final o de término emanado de la Agencia, sea ilegal y les cause perjuicio, podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante.

VI. Creación de nuevos órganos

Órgano de la Administración	Normativa	Objeto
Consejo Multisectorial sobre Ciberseguridad ("Consejo")	Párrafo 3°, del Título III de la LMC	Órgano de carácter consultivo y que tendrá por función asesorar y formular recomendaciones a la Agencia en el análisis y revisión periódico de la situación de ciberseguridad del país, en el estudio de amenazas existentes y potenciales en el ámbito de ciberseguridad, y proponer medidas para abordarlas.
Red de conectividad segura del Estado ("RCSE")	Párrafo 4°, del Título III de la LMC	Proveerá servicios de interconexión y conectividad a internet a los organismos de la Administración del Estado señalados en el artículo 1° de la presente ley.
Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional)	Párrafo 5°, del Título III de la LMC	Responder ante ciberataques o incidentes de ciberseguridad, cuando éstos sean de efecto significativo, y coordinar a los CSIRT que pertenezcan a organizamos de la Administración del Estado frente a ciberataques o incidentes de ciberseguridad de efecto significativo.
Equipo de respuesta a incidentes de seguridad informática de la Defensa Nacional ("CSIRT de la Defensa Nacional")	Título V de la LMC	Organismo responsable de la coordinación, protección y seguridad de las redes y sistemas del Ministerio de Defensa Nacional y de los servicios esenciales y operadores vitales para la defensa nacional, además de cumplir aquellas tareas que le sean encomendadas, con el propósito de resguardar la defensa y la seguridad nacional.
Comité Interministerial sobre Ciberseguridad	Título VIII de la LMC	Asesorar al Presidente de la República en materias de ciberseguridad relevantes para el funcionamiento del país.

VII. Disposiciones transitorias

En sus disposiciones transitorias, se faculta al Presidente de la República para que en el plazo de un año de publicada la LMC, establezca mediante decretos con fuerza de ley, las normas necesarias para regular la determinación de un periodo de vigencia de las normas establecidas por la LMC, el que no podrá ser inferior a seis meses desde su publicación.

CONTACTO

JUAN ENRIQUE ALLARD
Socio

jeallard@guerrero.cl

JOSÉ GABRIEL UNDURRAGA
Socio

jgundurraga@guerrero.cl

DIEGO MORANDÉ
Asociado Senior

dmorande@guerrero.cl

ROBERTO BURGOS
Asociado Senior

rburgos@guerrero.cl

VALENTINA MORA
Asociada Senior

vmora@guerrero.cl

JAVIERA GONZÁLEZ
Asociada

jgonzalezn@guerrero.cl