Alerta Legal

BOFILL MIR ABOGADOS

Promulgación de la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información

La ley establece exigencias en materia de ciberseguridad, una nueva institucionalidad y un nuevo régimen de infracciones por su infracción.

Manuel Bernet

Socio
Área IP, datos y tecnología

Jorge Tisné

Asociado Senior
Área IP, datos y tecnología

Santiago, 26 de marzo de 2024

Con fecha 26 de marzo de 2024, el Presidente de la República promulgó la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Por lo tanto, queda pendiente que la ley sea publicada en el Diario Oficial.

La ley establece diversos cambios y novedades en materia de ciberseguridad. A continuación, se enuncian algunos de los elementos más importantes.

I. Objetivo y principios

El objetivo de la ley es establecer 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. Asimismo, establece los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad, así como los deberes de las instituciones obligadas los mecanismos de control, supervisión, responsabilidad y sanción, entre otros.

La ley enumera una serie de principios y deberes que deben ser cumplidos por los sujetos obligados. Los principios enunciados en la ley son: (i) control de daños; (ii) cooperación con la autoridad; (iii) coordinación; (iv) seguridad en el ciberespacio; (v) respuesta responsable; (vi) seguridad informática; (vii) racionalidad; y (viii) seguridad y privacidad por defecto y desde el diseño.

II. Sujetos obligados

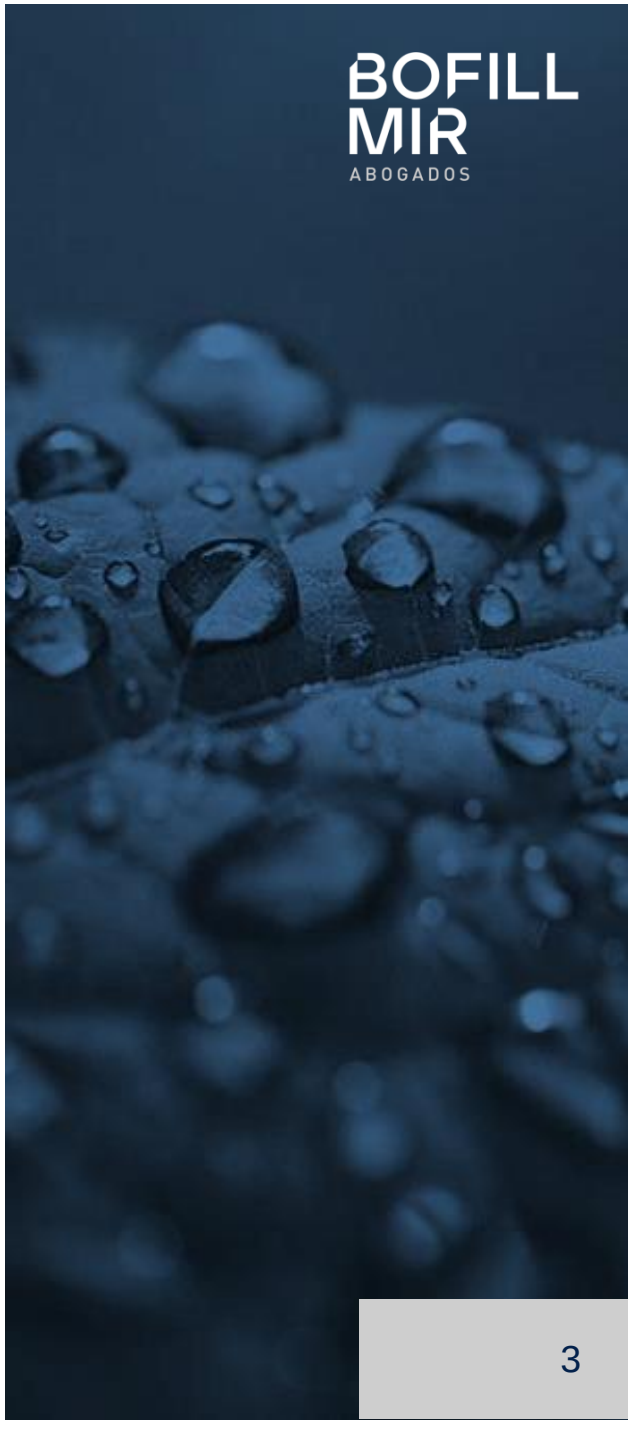
La ley aplicará a las instituciones que la nueva Agencia Nacional de Ciberseguridad califique como “Servicios Esenciales” y a aquellas calificadas como “Operadores de Importancia Vital”.

Son Servicios Esenciales:

- Los provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional;

- Los prestados bajo concesión de servicio público;

- Los proveídos por **instituciones privadas** que realicen actividades de **generación, transmisión o distribución eléctrica**; transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento; telecomunicaciones; **infraestructura digital**; servicios digitales, 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**.



II. Sujetos obligados

Son Operadores de Importancia Vital ("OIV"), quienes reúnan los siguientes requisitos:

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

- 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.

- Además la Agencia podrá calificar como OIV a instituciones privadas que reúnan los 2 requisitos anteriores y que cumplan con 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.

III. Deberes

Las instituciones obligadas por la ley deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad.

Entre las obligaciones más relevantes de los OIV se encuentra:

- Implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional del servicio.

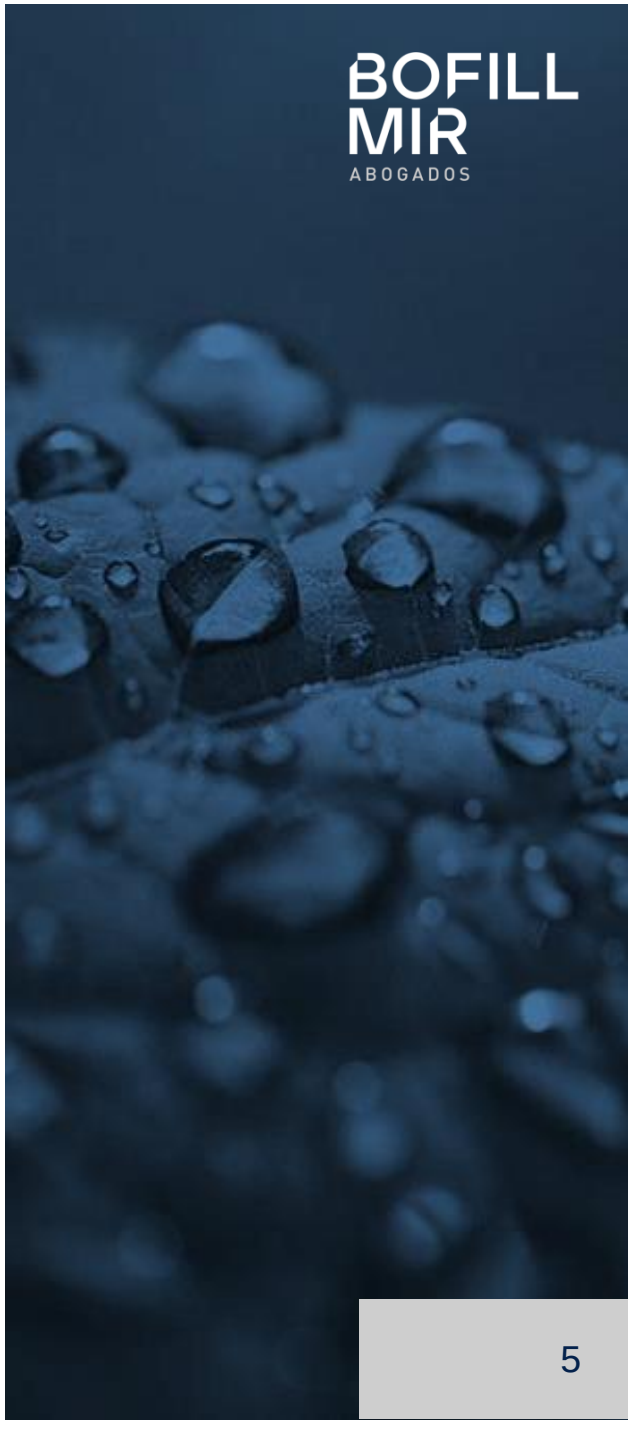
- Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de seguridad de la información, de conformidad a lo que señale el reglamento.

- Elaborar e implementar planes de continuidad operacional y ciberseguridad.

- Informar a los potenciales afectados, en la medida que puedan identificarse y cunado así lo requiera la Agencia, 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.

- Designar un delegado de ciberseguridad.

Además, todas las instituciones reguladas por la ley deberán **reportar** dentro de 3 horas al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos previstos en la ley.



IV. Nueva Institucionalidad

La ley crea una nueva institucionalidad que esté avocada a la al resguardo y promoción de la ciberseguridad en el país. Esta institucionalidad estará conformada principalmente por:

- Agencia Nacional de Ciberseguridad,
- Consejo Multisectorial sobre Ciberseguridad,
- Comité Interministerial sobre Ciberseguridad,
- Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT),
- CSIRT de la Defensa Nacional.

V. Agencia Nacional de Ciberseguridad

Esta Agencia tendrá por objeto asesorar al Presidente de la República en materias propias 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, promoción y respeto del derecho a la seguridad informática, coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

Esta nueva Agencia estará premunida de diversas atribuciones, entre las que destacan: (i) Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias en materia de ciberseguridad; (ii) Crear y administrar un Registro Nacional de Incidentes de Ciberseguridad; (iii) fiscalizar el cumplimiento de la ley; (iv) instruir el inicio de procedimientos sancionatorios y sancionar las infracciones e incumplimientos de los sujetos obligados.

VI. Infracciones y sanciones

La ley clasifica las distintas infracciones en leves, graves y gravísimas para todas las instituciones reguladas. Asimismo, se establecen sanciones específicas para OIV.

Las infracciones a la ley conllevarán la imposición de las siguientes multas:

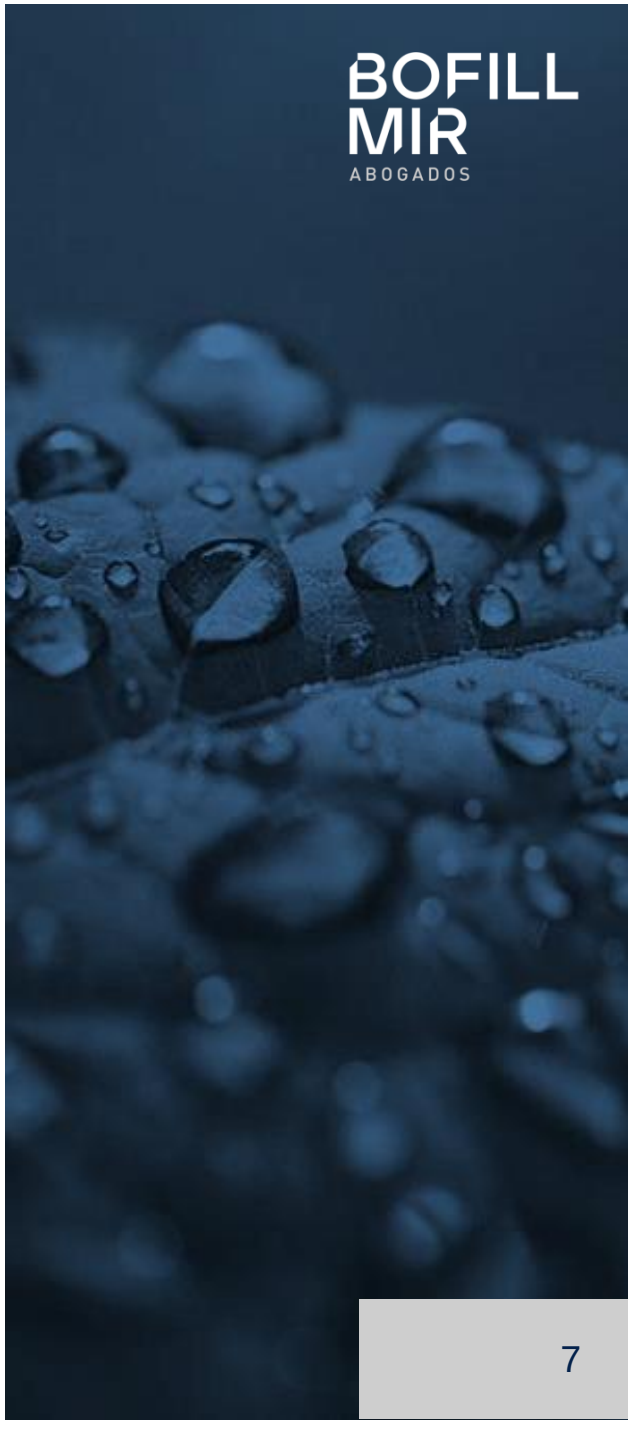
- Infracciones leves: Multa de hasta 5.000 UTM;

- Infracciones graves: Multa de hasta 10.000 UTM; e

- Infracciones gravísimas: Multa de hasta 20.000 UTM.

Las multas podrán llegar al doble en caso de tratarse de un Operador de Importancia Vital, pudiendo llegar a 40.000 UTM.

La multa será fijada teniendo en consideración el grado en que el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones, la probabilidad de ocurrencia del incidente, el grado de exposición del infractor a los riesgos, la gravedad de los efectos de los ataques incluidas sus repercusiones sociales o económicas, la reiteración en la infracción dentro del plazo de 3 años contado desde el momento en que se produjo el incidente, el tamaño y la capacidad económica del infractor.



VII. Entrada en vigencia de la ley

Una vez publicada la ley en el Diario Oficial, el Presidente de la República deberá en el plazo de 1 año expedir decretos con fuerza de ley para implementar la nueva normativa, incluyendo el plazo para el inicio de actividades de la nueva Agencia y determinar un periodo para la vigencia de la ley, el cual no podrá ser inferior a seis meses desde su publicación.

Esta alerta legal fue preparada por el equipo de IP, datos y tecnología de Bofill Mir Abogados con fines informativos generales y no debe ser considerada como asesoría legal.

En caso de preguntas o comentarios respecto de esta información, puedes comunicarte con nuestro equipo:

Manuel Bernet

Socio
Área IP, datos y tecnología

Jorge Tisné

Asociado Senior
Área IP, datos y tecnología

Tel. +56 2 2757 7600
www.bofillmir.cl

Av. Andrés Bello 2711, piso 8,
Las Condes | Santiago, Chile