ENERO 2024

# Se aprueba proyecto de ley que establece Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información

Con fecha 12 de diciembre de 2023 el Senado ha aprobado en tercer trámite el proyecto de ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información (en adelante, la "**Ley de Ciberseguridad**"), restando únicamente su publicación y promulgación en atención a que el Presidente de la República ha comunicado que no hará uso de la facultad que le confiere el inciso primero del artículo 73 de la Constitución Política de la Republica.

La Ley de Ciberseguridad tiene por objeto establecer la institucionalidad necesaria para robustecer la ciberseguridad, ampliar y fortalecer el trabajo preventivo, la formación de una cultura pública en materia de seguridad digital, enfrentar las contingencias en el sector público y privado, y resguardar la seguridad de las personas en el ciberespacio.

De esta forma, la Ley de Ciberseguridad define los requisitos mínimos para la prevención y respuesta ante incidentes de seguridad informática, establece parámetros para determinar qué constituye infraestructura crítica de la información, y las obligaciones que esto involucra para los órganos que la tengan a cargo, junto con la competencia de los entes fiscalizadores sobre sus sectores regulados.

## 1. Sujetos Pasivos – Entes y empresas obligados.

La Ley de Ciberseguridad y sus obligaciones serán aplicables a aquellas instituciones que presten servicios calificados como esenciales, los cuales son definidos como los servicios prestados por organismos de la administración del Estado y por el Coordinador Eléctrico Nacional, aquellos prestados bajo concesión de servicio público, y los provistos por instituciones privadas que realicen ciertas actividades establecidas en la misma ley, entre las cuales se incluyen las siguientes:

1. Generación, transmisión y distribución eléctrica;
2. Transporte, almacenamiento o distribución de combustible;
3. Suministros de agua potable o saneamiento;
4. Telecomunicaciones;
5. Infraestructura digital;
6. Servicios digitales;
7. Transporte terrestre, aéreo, ferroviario o marítimo y la operación de su infraestructura respectiva
8. Banca, servicios financieros y medios de pago; Prestaciones institucionales públicas y privadas de salud.

Asimismo, la Agencia Nacional de Ciberseguridad (en adelante, "**Agencia**") podrá calificar otros servicios como esenciales mediante resolución fundada 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.

Finalmente, la Ley de Ciberseguridad se aplicará también a los Operadores de Importancia Vital (en adelante, "**OIV**"), cuya calificación podrá ser otorgada por la Agencia mediante resolución tanto a prestadores de servicios esenciales como a aquellos no esenciales, siempre que se cumplan los requisitos específicos establecidos en el artículo 5° de la ley.

ENERO 2024

## 2. Obligaciones.

La Ley de Ciberseguridad establece diversas obligaciones para las instituciones ya mencionadas, destacando las siguientes:

1. Aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad.
2. Implementación 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.
3. Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de seguridad de la información.
4. Elaborar e implementar planes de continuidad operacional y ciberseguridad.
5. 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 CSIRT Nacional.
6. Adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad, incluida la restricción de uso o el acceso a sistemas informáticos.
7. Informar a los potenciales afectados, en la medida que puedan identificarse y cuando 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.
8. Contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene.
9. Designar un delegado de ciberseguridad.
10. Obligación de reportar: Todos los prestadores de Servicios Esenciales y OIV tendrán la obligación de reportar al CSIRT Nacional los casos de incidentes de ciberseguridad que puedan tener efectos significativos.

## 3. Ente regulador.

La Ley de Ciberseguridad establece la creación de la Agencia Nacional de Ciberseguridad, la cual tiene como fin asesorar al Presidente en la protección del ciberespacio nacional y coordinar las distintas instituciones a cargo de la ciberseguridad del país. También propone la creación de entes como el Consejo Multisectorial sobre Ciberseguridad, el Equipo de Respuesta a Incidentes de Seguridad Informática (en adelante, el "**CSIRT**") y el CSIRT Nacional.

El Consejo Multisectorial Sobre Ciberseguridad es un consejo de carácter consultivo, que tendrá como función asesorar y formar recomendaciones a la Agencia en el análisis periódico de la situación de ciberseguridad del nivel nacional; así como también aspectos políticos y técnicos y la manera en que se coordinan.

El CSIRT Nacional es el órgano encargado del reporte frente a ciberataques o incidentes informáticos ocurridos en el caso sea el caso significativo.

## 4. Sanciones.

La Ley de Ciberseguridad clasifica las distintas infracciones en leves, graves y gravísimas. Las infracciones a la ley conllevarán la imposición de las siguientes multas:

1. Infracciones leves: Multa de hasta 5.000 UTM;
2. Infracciones graves: Multa de hasta 10.000 UTM; e
3. Infracciones gravísimas: Multa de hasta 20.000 UTM.

Las multas podrán llegar al doble en caso de tratarse de un OIV (hasta 40.000 UTM).

## 5. Vigencia de la Ley de Ciberseguridad.

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

---

## EQUIPO DE CONTACTO

Juan José Prieto U. jjprieto@moralesybesa.cl +(56) 224727051

Raimundo Hurtado P.

Sebastián Romero F.