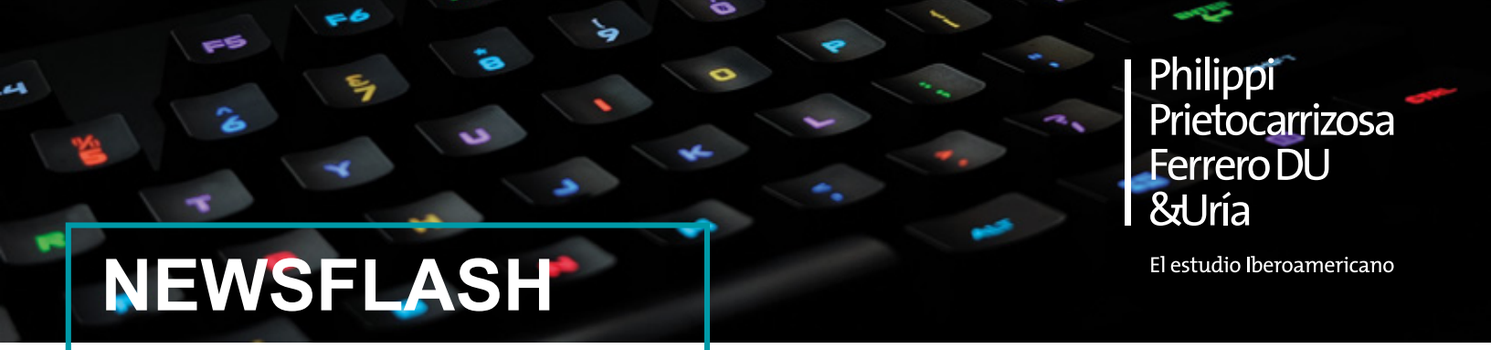

Philippi Prietocarrizosa Ferrero DU & Uría

El estudio Iberoamericano

NEWSFLASH

DERECHO PÚBLICO

LEY MARCO DE CIBERSEGURIDAD

Con fecha 8 de abril de 2024 se publicó en el Diario Oficializa la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información[1] (la "**Ley**").

Esta ley establece nuevas exigencias en materia de ciberseguridad para los organismos del Estado calificadas como *"esenciales"*, nuevas instituciones y, además, un nuevo régimen de infracciones.

1. OBJETO DE LA LEY Y DISPOSICIONES GENERALES

El artículo 1° de la mentada ley tiene por objeto establecer la institucionalidad y la normativa general que permitan regular, coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares. Además, dispone los requisitos mínimos para la prevención y contención de incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones determinadas en el artículo 4°, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

Por su parte, en el artículo 3° se enumeran una serie de principios rectores que se deberán observar en la aplicación de la ley[2]. En cuanto al ámbito de acción de la ley, el artículo 1 inciso tercero establece que serán aplicables a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio.

El artículo 4° delimitada el ámbito de vigor, estableciendo que se aplicará a instituciones que presten servicios calificados como esenciales y a aquellas que sean calificadas como operadores de importancia virtual. A continuación, se establece que se entiende por "servicio esencial" y "operador 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:
  a. Generación, transmisión o distribución eléctrica;
  b. Transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento;
  c. Telecomunicaciones;
  d. Infraestructura digital;
  e. Servicios digitales, servicios de tecnología de la información gestionados por terceros;
  f. Transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva;
  g. Banca, servicios financieros y medios de pago;
  h. Administración de prestaciones de seguridad social; servicios postales y de mensajería;
  i. Prestación institucional de salud por entidades tales como hospitales, clínicas, consultorios y centros médicos;
  j. Producción y/o investigación de productos farmacéuticos.

Son Operadores de Importancia Vital, quienes cumplan con 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 Operador de Importancia Vital 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.

[1] Cámara de Diputadas y diputados, boletín 14847.

[2] (1) Principio de control de daños; (2) Principio de cooperación con la autoridad; (3) Principio de coordinación según lo dispuesto en el artículo 5° inciso segundo de la ley N°18.575; (4) Principio de seguridad en el ciberespacio; (5) Principio de respuesta responsable; (5) Principio de respuesta responsable; (6) Principio de seguridad informática; (7) Principio de racionalidad y (8) Principio de seguridad y privacidad

2. OBLIGACIONES DE CIBERSEGURIDAD

La Ley distingue entre deberes generales en el que las instituciones deberán aplicar de manera permanente y deberes específicos que deben cumplir las entidades calificadas como Operadores de Importancia Vital.

El artículo 7° de la ley establece que las instituciones obligadas deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Por su parte, el artículo 8° enumera una serie de deberes específicos que los Operadores de Importancia Vital deberán cumplir, entre ellos se encuentra la obligación de implementar sistemas de gestión de seguridad de la información continuos; elaborar y mantener planes de continuidad operacional y ciberseguridad, los que deberán certificarse y someterse a revisiones periódicas; realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y sistemas; informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos; designar un delegado de ciberseguridad, entre otros.

3. AGENCIA NACIONAL DE CIBERSEGURIDAD

El artículo 10° 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 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, y coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

En cuanto a sus atribuciones, las principales consisten en: asesorar al Presidente de la República en la elaboración y aprobación de la Política Nacional de Ciberseguridad; dictar protocolos y estándares, instrucciones generales y particulares para las instituciones obligadas por la presente ley; aplicar e interpretar las disposiciones legales y reglamentarias en materia de ciberseguridad; coordinar y supervisar al CSIRT; crear y administrar un Registro Nacional de Incidentes de Ciberseguridad; calificar a los servicios esenciales y a los operadores de importancia vital; requerir a las entidades obligadas por la presente ley que hayan visto afectados sus servicios por un incidente de ciberseguridad, que entreguen a los potenciales afectados información veraz y oportuna sobre su ocurrencia, entre otras atribuciones.

Por otro lado, la dirección y administración superior de la Agencia estará a cargo de un Director o Directora Nacional, quien será el jefe superior del Servicio, tendrá la representación legal, judicial y extrajudicial del mismo y será designado conforme a las normas del Sistema de Alta Dirección Pública establecidas en la ley N°19.882.

4. EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE LA DEFENSA

Adicionalmente, la Ley crea el Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa -CSIRT-, dependiente del Ministerio de Defensa Nacional, siendo el organismo 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, con el propósito de resguardar la defensa y la seguridad nacional.

5. INFRACCIONES Y SANCIONES

El artículo 37° dispone que la autoridad sectorial será competente para fiscalizar, conocer y sancionar las infracciones, así como ejecutar las sanciones según lo establece la normativa de ciberseguridad. Le corresponderá a la Agencia fiscalizar, conocer y sancionar las infracciones, así como ejecutar las sanciones.

La Ley clasifica a las infracciones en leves, graves y levísimas, y además, prevé infracciones específicas para los operadores de importancia vital.

Las infracciones conllevarán la imposición de las siguientes multas:

- Infracciones leves: Multa de hasta 5.000 UTM;[3]
- Infracciones graves: Multa de hasta 10.000 UTM[4]; e
- Infracciones gravísimas: Multa de hasta 20.000[5] UTM.

Las multas podrán llegar al doble en caso de tratarse de un Operador de Importancia Vital, pudiendo llegar a 40.000 UTM[6].

[3]Equivalentes a $346,344 USD, aproximadamente.
[4]Equivalentes a $692,688 USD, aproximadamente.
[5]Equivalente a 1,385,377 USD, aproximadamente.
[6]Equivalente a 2,770,754 USD, aproximadamente.

NEWSFLASH

DERECHO PÚBLICO

6. BENEFICIOS DE LA LEY

La Ley tiene por propósito establecer la institucionalidad necesaria para robustecer la ciberseguridad, fortalecer el trabajo preventivo, además de propender a la formación de una cultura pública en materia de seguridad digital. Para ello, se plantea fortalecer la institucionalidad, otorgando protección ante incidentes de ciberseguridad en distintos ámbitos.

En primer lugar, se protegerá al Estado, sus redes y los sistemas informáticos, e infraestructura de la información del sector público, especialmente, aquellas que son esenciales y críticas para los ciudadanos.

En segundo lugar, se protegerá la seguridad nacional, promoviendo el resguardo de datos, las redes y los sistemas informáticos e infraestructura de la información del sector privado, especialmente aquellas que son esenciales para el adecuado funcionamiento del país, velando y asegurando la continuidad operacional de las infraestructuras críticas de la información del país.

A su vez, se pretende prevenir ciber amenazas al mejorar las instancias de comunicación, coordinación y colaboración entre diversas instituciones, organizaciones y empresas, tanto del sector público como privado, nacionales e internacionales, con el propósito de fortalecer la confianza y entregar una respuesta común a los riesgos que se presentan en el ciberespacio, previniendo el fenómeno del ciberataque y evitando la expansión de los efectos perjudiciales de un incidente de ciberseguridad.

Por último, la normativa establece que se gestionarán los riesgos del ciberespacio, lo que permitirá identificar las vulnerabilidades, amenazas y riesgos en el uso, procesamiento, almacenamiento y transmisión de la información.[7]

7. DESAFIOS DE LA ENTRADA EN VIGOR DE LA LEY

Esta Ley entrará en vigor de forma diferida, ofreciendo a las empresas e instituciones un período de transición para adaptarse a estas nuevas disposiciones.

Finalmente, resulta fundamental que las empresas e instituciones realicen un análisis sobre los siguientes puntos:

a. Determinen si están sujetas o no a la Ley.

b. Comprendan las implicancias de la misma.

c. Analicen la situación institucional y su estatus de cumplimiento, determinando qué pasos deben seguir para cumplir con los objetivos.

d. Comiencen a ajustar sus políticas y protocolos de seguridad informática para alinearse con los requisitos establecidos.

e. Avancen en la formación de su personal y en la sensibilización en materia de ciberseguridad.

Lo anterior permitirá a los sujetos obligados adaptarse a los requerimientos de la nueva normativa, evitando multas y mejorando su exposición a ataques informáticos mediante la creación de un entorno digital seguro y resiliente[8].

Para mayor información contactar a:

José Luis Lara

Socio Derecho Público
joseluis.lara@ppulegal.com

Florencia Portales

Asociada Principal Derecho Público
florencia.portales@ppulegal.com

[7] Proyecto de ley establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. - Diario Constitucional
[8] Nueva Ley Marco de Ciberseguridad: lo que debes saber en 1 minuto. Disponible en: https://altlegal.cl/nueva-ley-marco-de-ciberseguridad-lo-que-debes-saber-en-1-minuto/