04 de abril de 2024

Se publica en el Diario Oficial la Ley Marco sobre Ciberseguridad

Con fecha 8 de abril de 2024, se publicó en el Diario Oficial la Ley 21.663 Marco sobre Ciberseguridad (la "Ley"), tras haber sido promulgada por el Presidente de la República el pasado 26 de marzo.

La nueva Ley supone la implementación de aspectos y cambios relevantes en materia de ciberseguridad, lo que conlleva una serie de efectos y consecuencias, los que se detalla a continuación:

I. *La Ley: Cinco puntos para tener en cuenta*

1.-Nueva institucionalidad

En primer término, la Ley implementa una nueva institucionalidad en la materia, al crear la (i) *Agencia Nacional de Ciberseguridad* ("ANCI"); el (ii) *Consejo Multisectorial sobre Ciberseguridad* ("Consejo"); (iii) *el Comité Interministerial sobre Ciberseguridad* ("Comité"); y los (iv) *Equipos de Respuesta a Incidentes de Seguridad Informática* (cada uno, "CSIRT"), entre los que se encuentran el CSIRT Nacional, el CSIRT de la Defensa Nacional y otros CSIRT de organismos de la Administración del Estado.

En lo que refiere a la **ANCI**, corresponderá a un servicio público descentralizado, de carácter técnico y especializado, cuyos objetivos principales serán asesorar al Presidente de la República en materias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar a las distintas instituciones con competencia en ciberseguridad, velar por la protección, promoción y respecto de la seguridad informática, entre otros.

Para dar cumplimiento a los objetivos señalados, la ANCI tendrá diversas atribuciones, entre las que se encuentran, (i) **facultades normativas**; (ii) **facultades fiscalizadoras**; y (iii) **facultades sancionatorias**; entre otras.

Asimismo, la Ley incluye un mecanismo de coordinación regulatoria entre la ANCI y entidades sectoriales cuando los protocolos, estándares técnicos o instrucciones que la ANCI emita en el ejercicio de sus funciones impacten las áreas de competencia de esas entidades. Además, las autoridades sectoriales podrán emitir normativas generales, técnicas e instrucciones para fortalecer la ciberseguridad en las instituciones de su sector, en cumplimiento de la regulación correspondiente y en colaboración con la ANCI.

2.- Principios que rigen la regulación en materia de ciberseguridad

La Ley introduce varios principios que las instituciones obligadas (indicadas en el punto 3 siguiente) deberán observar en su conducta. Entre estos principios se encuentran: (i) control de daños; (ii) coordinación con la autoridad; (iii) respuesta responsable; (iv) seguridad informática; (v) racionalidad; y (vi) seguridad y privacidad por defecto y desde el diseño.

Carey y Cía. Ltda.
Isidora Goyenechea 2800, Piso 43
Las Condes, Santiago, Chile.
www.carey.cl

3.- Ámbito de aplicación

En cuanto a su ámbito de aplicación, la Ley aplicará a instituciones prestadoras de **servicios calificados como "Esenciales"**, por un lado, y a aquellas calificadas como **Operadores de Importancia Vital**, por otro.

En cuanto a los Servicios Esenciales, estos corresponden a:

1. Aquellos provistos por organismos de la Administración del Estado y el Coordinador Eléctrico Nacional.
2. Aquellos prestados bajo concesión de derecho público.
3. Aquellos provistos por instituciones privadas, que realicen las siguientes actividades:
    a. Generación, transmisión o distribución eléctrica;
    b. Transporte, almacenamiento o distribución de combustibles;
    c. Suministro de agua potable o saneamiento;
    d. Telecomunicaciones;
    e. Infraestructura digital;
    f. Servicios digitales y tecnología de la información gestionados por terceros;
    g. Transporte terrestre, aéreo, ferroviario o marítimo;
    h. Banca, servicios financieros y medios de pago;
    i. Administración de prestaciones de seguridad social;
    j. Servicios postales y mensajería;
    k. Prestación institucional de salud (hospitales, clínicas, etc.); y
    l. Producción y/o investigación de productos farmacéuticos.
4. Otros servicios que la ANCI en futuro pueda calificar como "Esenciales" mediante resolución fundada del o la Directora 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, de la Administración del Estado, a la defensa nacional, o a la seguridad y el orden público.

Asimismo, corresponderá a la misma ANCI la determinación de aquellas instituciones prestadoras de Servicios Esenciales que califiquen como Operadores de Importancia Vital, mediante resolución, cuando la institución reúna los requisitos de: *i) proveer un servicio que dependa de redes y sistemas informáticos;* y *ii) la afectación, interceptación, interrupción o destrucción de sus servicios suponga 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*.

Del mismo modo, la ANCI estará facultada para calificar como Operador de Importancia Vital a instituciones privadas que, aunque no tengan la calidad de prestadores de Servicios Esenciales, reúnan los requisitos establecidos en el párrafo anterior, y bajo determinados supuestos.

4.- Obligaciones de ciberseguridad

En cuanto a las obligaciones que contempla la Ley, por un lado, están los **deberes generales**, aplicables tanto a prestadores de Servicios Esenciales como aquellos considerados Operadores de Importancia Vital, los cuales se encuentran obligados a:

1. **Deber de reportar al CSIRT Nacional de los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos** en los términos de la Ley, tan pronto les sea posible, dentro de un plazo máximo de tres horas, y de conformidad a los demás criterios y formalidades que establece la Ley.

2. **Deber de aplicar permanentemente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad**, lo que exige la implementación de los protocolos y estándares establecidos por la ANCI, y la regulación sectorial respectiva.

Por otro lado, la Ley introduce **deberes específicos para Operadores de Importancia Vital**, quienes estarán obligados, entre otros deberes, a lo siguiente:

1. Implementar un sistema de gestión de seguridad de la información;
2. Elaborar e implementar planes de continuidad operacional y ciberseguridad;
3. Realizar operaciones de revisión, ejercicios, simulacros y análisis de las redes y sistemas informáticos que comprometan la ciberseguridad;
4. Adoptar las medidas necesarias para reducir el impacto y propagación de un incidente de ciberseguridad;
5. Obtener las certificaciones de ciberseguridad que dispone la Ley; y
6. Contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, incluyendo campañas de ciberhigiene.

5- Infracciones y sanciones asociadas

La Ley prevé diversas sanciones por el incumplimiento de sus disposiciones, las que se clasifican en 3 categorías: **leves**, **graves** y **gravísimas**.

A modo meramente ejemplar, la ley considerará como **leve** la entrega fuera de plazo de la información requerida por la ANCI que no sea necesaria para la gestión de un incidente de ciberseguridad, como **grave** el incumplir con la obligación de reportar y como infracción **gravísima**, el entregar información manifiestamente falsa o errónea a la ANCI, y que esta haya sido necesaria para la gestión de un incidente de ciberseguridad.

La Ley contempla además infracciones y sanciones específicas ante la inobservancia de los deberes específicos de los Operadores de Importancia Vital.

En cuanto a las sanciones que contempla la Ley, éstas se traducen en la imposición de una multa a beneficio fiscal:

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.

En el caso de Operadores de Importancia Vital, estas multas pueden incluso llegar hasta el doble.

II. *Próximos pasos y entrada en vigencia (lo que viene)*

Por último, en cuanto a la entrada en vigor de la Ley, corresponderá al Presidente de la República expedir, en un plazo de un año contados desde la publicación en el Diario Oficial, uno o varios decretos con fuerza de ley, los que establecerán el período de vacancia antes de la entrada en vigencia de las disposiciones de la Ley (que no podrá ser menor a seis meses a partir de su publicación), así como la fecha de inicio de las actividades de la ANCI, entre otros aspectos relevantes.

AUTORES: *Guillermo Carey, José Ignacio Mercado, Stefano De Cristofaro, Iván Meleda. Ricardo Alonso*