ALERTA LEGAL

ALERTA LEGAL ENTRADA EN VIGENCIA LEY N° 21.663 MARCO DE CIBERSEGURIDAD.

27_12_2024

Cariola Díez Pérez-Cotapos

Alerta legal entrada en vigencia Ley N° 21.663 marco de ciberseguridad.

El 24 de diciembre de 2024 se publicó en el Diario Oficial el Decreto con Fuerza de Ley 1-21.663 (DFL 1) del Ministerio del interior y Seguridad Pública, que establece la entrada en vigencia de la Ley Nº 21.663 marco de ciberseguridad (LMC).

Así, el cronograma de puesta en marcha es el siguiente:

1° de enero de 2025: Inicio de actividades de la Agencia Nacional de Ciberseguridad (ANCI) y entrada en vigencia de las normas de la LMC.

1° de marzo de 2025: Entran en vigencia las siguientes normas:

- Determinación de Operadores de Importancia Vital (OIV): La ANCI identificará los Prestadores de Servicios Esenciales (PSE) que serán considerados OIV.
- Deberes específicos aplicables a los OIV.
- Deber de PSE y OIV de reportar incidentes: Obligación de reportar al CSIRT Nacional, dentro de un plazo máximo de tres horas, los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos.
- Infracciones y sanciones.

Prestadores de Servicios Esenciales (PSE)

La LMC establece que son PSE:

a) los Organismos de la Administración del Estado y el Coordinador Eléctrico Nacional**;**

b) los Concesionarios de servicios públicos; y

c) Las instituciones privadas que realicen las siguientes actividades:

i) generación, transmisión o distribución eléctrica;

ii) transporte, almacenamiento o distribución de combustibles;

iii) suministro de agua potable o saneamiento;

iv) telecomunicaciones;

v) infraestructura digital;

vi) servicios digitales y de tecnología de la información gestionados por terceros;

vii) transporte terrestre, aéreo, ferroviario o marítimo, y la operación de su infraestructura;

viii) banca, servicios financieros y medios de pago;

ix) administración de prestaciones de seguridad social;

x) servicios postales y de mensajería;

xi) prestación institucional de salud, incluyendo hospitales, clínicas, consultorios y centros médicos; y

xii) producción y/o investigación de productos farmacéuticos.

Alerta legal entrada en vigencia Ley N° 21.663 marco de ciberseguridad.

Obligaciones PSE

a) implementación de los protocolos y estándares establecidos por la ANCI -los cuales aún no se dictan- así como de los estándares particulares de ciberseguridad dictados de conformidad a la regulación sectorial respectiva, si existiesen, y

b) reportar al CSIRT Nacional, en un plazo máximo de 3 horas, ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos. Esta obligación entrará en vigencia el 01 de marzo de 2025 y, asimismo, requiere un reglamento que operativice su funcionamiento el cual se encuentra en proceso de toma de razón ante Contraloría General de la República (CGR) bajo el número 295/2024.

Operadores de Importancia Vital (OIV)

Un PSE eventualmente podrá ser designada como OIV, mediante resolución fundada del director de la ANCI. Para ello se solicitará informes a los organismos públicos con competencia sectorial sobre las instituciones privadas que puedan ser calificadas como OIV. Posteriormente, se elaborará una nómina preliminar, la cual será sometida a consulta pública durante 30 días. Finalizada esta etapa, la ANCI contará con 30 días adicionales para preparar el informe final con la nómina definitiva. Contra esta resolución podrán interponerse los recursos administrativos establecidos en la Ley Nº 19.880, y el especial del artículo 46 de la LMC.

Adicionalmente, se requiere un reglamento que regule los detalles necesarios para la correcta ejecución del procedimiento, el cual se encuentra en proceso de toma de razón ante la CGR bajo el número 285/2024.

Obligaciones OIV

Además de las obligaciones establecidas para los PSE se suman las siguientes obligaciones específicas:

a) implementar un sistema continuo de gestión de seguridad de la información, evaluando riesgos, probabilidades e impactos de incidentes de ciberseguridad;

b) mantener un registro detallado de las acciones ejecutadas en dicho sistema;

c) desarrollar e implementar planes de continuidad operacional y ciberseguridad, certificados cada dos años o con mayor frecuencia si la ANCI lo instruye fundadamente;

d) realizar revisiones, ejercicios y simulacros periódicos para detectar y reportar amenazas al CSIRT Nacional;

e) adoptar medidas rápidas y efectivas para mitigar el impacto y la propagación de incidentes;

f) contar con las certificaciones exigidas por la LMC, cuyo reglamento aún no se ha emitido;

g) informar, si la ANCI lo requiriese, a los potenciales afectados sobre ciberataques que puedan comprometer gravemente su información, especialmente si involucran datos personales;

h) implementar programas de capacitación continua para trabajadores y colaboradores; e

i) designar un delegado de ciberseguridad que actúe como contraparte de la ANCI y reporte a las autoridades superiores de la Compañía.

Alerta legal entrada en vigencia Ley N° 21.663 marco de ciberseguridad.

Tales deberes sólo serán exigibles a partir del 01 de marzo de 2025 y su aplicación a la institución privada supone que ella ha sido designada OIV en base al procedimiento antes señalado.

Sanciones

La LMC distingue entre infracciones leves, graves y gravísimas, las que prescriben en 3 años. Las multas llegan hasta las 20.000 UTM (app USD 1.350.000) para los PSE y 40.000 UTM (app USD 2.700.000) para las OIV. El régimen infraccional de la LMC entrará en vigencia el próximo 01 de marzo de 2025.

Contactos:

Carolina Flisfisch
Socia

Eduardo Vilches
Asociado Senior

Gabriel Pensa
Asociado Senior