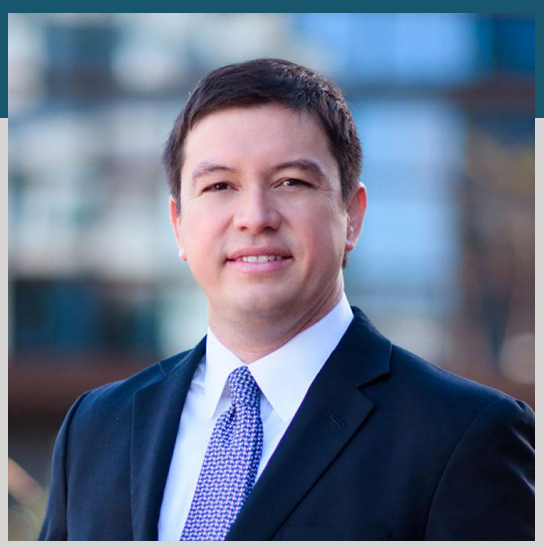
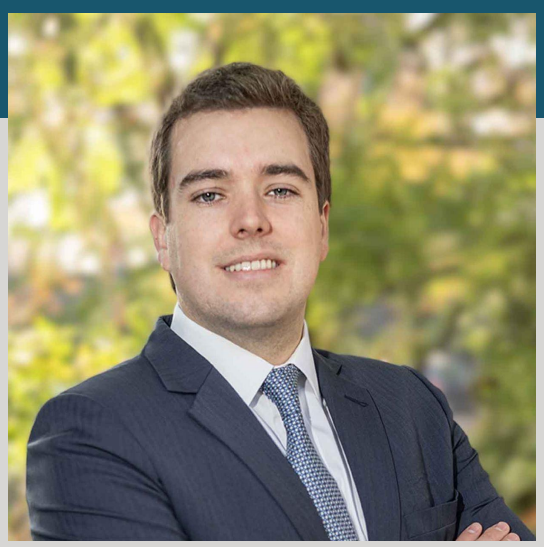
#ClavesLembeye2024

Las Claves de la Ley Marco sobre Ciberseguridad

Con fecha 8 de abril fue publicada en el Diario Oficial la ley N° 21.663 denominada Ley Marco sobre Ciberseguridad (la "**LMC**").



Jorge Lembeye
SOCIO LEMBEYE



Reginald Horn
ASOCIADO

LEMBEYE

Para más información, ponerse en contacto:

Jorge Lembeye
jlembeye@lembeye.cl
+56 9 8288 6928

Reginald Horn
rhorn@lembeye.cl
+56 9 8240 8924

Objetivos.

La LMC tiene por objetivos principales establecer:

- La institucionalidad, principios y normativa general con respecto a las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares.
- Requisitos mínimos para prevenir, contener, resolver y dar respuesta a incidentes de ciberseguridad.
- Las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones que presten servicios “esenciales” y aquellas calificadas como operadores de “importancia vital” (artículos 4° a 6° de la LMC).
- Los mecanismos de control ante infracciones a la LMC.

En definitiva, la LMC busca garantizar un *nivel común y elevado de seguridad* tanto de las redes como de los *sistemas de información* utilizados para la provisión de los denominados *servicios esenciales*, mediante el establecimiento de mecanismos que permitan mejorar la protección frente a las amenazas que afectan a dichas redes y sistemas.

Mecanismos para asegurar dichos objetivos.

Los mecanismos que contempla la LMC y que permitirán mejorar la protección ante las amenazas de ciberseguridad corresponden a:

- Establecimiento de una institucionalidad robusta compuesta por la Agencia Nacional de Ciberseguridad (la “**Agencia**”), la cual tendrá facultades normativas, fiscalizadoras y sancionatorios. Además, se contempla el Consejo Multisectorial, el Comité Interministerial de Ciberseguridad, el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT) Nacional, de Defensa y de organismos de la Administración del Estado
- La aplicación de determinados principios y obligaciones que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los actores que prestan los servicios esenciales.

Francisco de Aguirre N°3720, piso 4, Vitacura, Santiago, Chile +56 (2) 3263 76 80

LEMBEYE

Para más información, ponerse en contacto:

Jorge Lembeye
jlembeye@lembeye.cl
+56 9 8288 6928

Reginald Horn
rhorn@lembeye.cl
+56 9 8240 8924

Francisco de Aguirre N°3720, piso 4, Vitacura, Santiago, Chile +56 (2) 3263 76 80

SUJETOS OBLIGADOS POR LA LMC.

¿A quiénes aplica la LMC? ¿Aplica a entidades privadas?

La LMC aplica tanto al sector público como al sector privado, en la medida que el organismo público o la empresa respectiva califiquen como prestador de *Servicios Esenciales* (**"Servicios Esenciales"**) u *Operadores de Importancia Vital* (**"OIV"**). También aplica a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio, todo lo anterior de conformidad con lo dispuesto en los artículos 5° y 6° de la LMC.

¿Quiénes prestan Servicios Esenciales?

La LMC señala en su Art. 4° que son Servicios Esenciales:

- Aquellos prestados por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional.
- Servicios prestados bajo concesión de servicio público.
- Servicios prestados por instituciones privadas que realicen las siguientes actividades: generación, transmisión o distribución eléctrica; transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento; telecomunicaciones; infraestructura digital; servicios digitales y 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.

Lo anterior es sin perjuicio de que la Agencia pueda calificar otros Servicios Esenciales mediante resolución fundada del Director 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 y/o de la Administración del Estado, a la defensa nacional, o a la seguridad y el orden público.

Para más información, ponerse en contacto:

Jorge Lembeye
jlembeye@lembeye.cl
+56 9 8288 6928

Reginald Horn
rhorn@lembeye.cl
+56 9 8240 8924

Francisco de Aguirre N°3720, piso 4, Vitacura, Santiago, Chile +56 (2) 3263 76 80

¿Quiénes son Operadores de Importancia Vital?

Un prestador de Servicios Esenciales puede además ser designado como OIV, cuando reúna los siguientes requisitos copulativos:

- Que de la provisión de dicho servicio dependa de las redes y sistemas informáticos.
- Que la afectación, interceptación, interrupción o destrucción del servicio respectivo 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.

Adicionalmente, la Agencia podrá calificar como OIV aquellas empresas privadas que, no teniendo la calidad de prestadores de Servicios Esenciales, reúnan los requisitos anteriores, y cuya calificación sea indispensable por haber adquirido un rol crítico o por su grado de exposición a los riesgos y las probabilidades de incidentes de ciberseguridad, teniendo en cuenta su gravedad y las consecuencias sociales y económicas asociadas.

La Agencia por medio de resolución fundada determinará los OIV, y para hacer dicha calificación, debe considerar el tamaño de las empresas, conforme a las normas especiales establecidas para las empresas de menor tamaño. Dicha resolución será reclamable conforme al procedimiento que expresa la misma ley.

DEBERES GENERALES Y ESPECÍFICOS QUE IMPONE LA LMC.

¿Cuáles son las obligaciones que poseen los prestadores de Servicios Esenciales?

Las empresas calificadas como prestadoras de Servicios Esenciales están sujetas al cumplimiento del deber general de aplicar en sus procesos organizacionales internos y de manera permanente, *los protocolos y estándares tecnológicos, organizacionales, físicos o informativos,* cuyo objetivo sea prevenir, reportar y resolver incidentes de ciberseguridad, conforme a lo que disponga la Agencia.

LEMBEYE

Para más información, ponerse en contacto:

Jorge Lembeye
jlembeye@lembeye.cl
+56 9 8288 6928

Reginald Horn
rhorn@lembeye.cl
+56 9 8240 8924

Deber de reportar: obligación común para todas las organizaciones reguladas por la LMC.

Todas las organizaciones que se encuentren reguladas por la LMC tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener *efectos significativos*, tan pronto les sea posible y conforme al cronograma que fija la misma ley.

¿Qué se entiende por incidente de efectos significativos?

Se entiende que un incidente de ciberseguridad tiene efecto significativo si es capaz de interrumpir la continuidad de un *servicio esencial* o afectar la *integridad física* o *la salud de las personas*, así como en el caso de afectar *sistemas informáticos* que contengan *datos personales*.

Para determinar la importancia de los efectos de un incidente, se tendrán especialmente en cuenta el número de personas afectadas, la duración del incidente y la extensión geográfica con respecto a la zona afectada por el incidente.

El *procedimiento específico* para notificar un incidente de ciberseguridad, la forma, así como las condiciones de anonimato, la taxonomía del informe y la periodicidad, serán establecidos en el reglamento de la ley.

¿Cuáles son las obligaciones específicas que poseen las empresas calificadas como OIV?

Además de cumplir con el deber general antes señalado, todos los OIV deberán, entre otras obligaciones:

- 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.
- Elaborar e implementar planes de continuidad operacional y ciberseguridad.

Francisco de Aguirre N°3720, piso 4, Vitacura, Santiago, Chile +56 (2) 3263 76 80

Para más información, ponerse en contacto:

Jorge Lembeye
jlembeye@lembeye.cl
+56 9 8288 6928

Reginald Horn
rhorn@lembeye.cl
+56 9 8240 8924

- Elaborar e implementar planes de continuidad operacional y ciberseguridad.
- 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.

INSTITUCIONALIDAD ESTABLECIDA EN LA LMC.

Agencia Nacional de Ciberseguridad.

La Agencia Nacional de Ciberseguridad es un servicio público de carácter técnico y especializado y tendrá atribuciones tales como:

- Dictar protocolos, estándares e instrucciones a que deberán ceñirse los Servicios Esenciales.
- Fiscalizar el cumplimiento de las disposiciones de la LMC y sus reglamentos, y de los protocolos, estándares técnicos e instrucciones generales y particulares dictados por ella.
- Instruir el inicio de procedimientos sancionatorios y sancionar las infracciones e incumplimientos en que incurran las instituciones obligadas.

En relación con este último punto, las autoridades sectoriales (i.e. Comisión para el Mercado Financiero), seguirán siendo competentes para fiscalizar, conocer y sancionar las infracciones y ejecutar las sanciones, adecuándose a lo establecido en la LMC.

CSIRT Nacional.

Dentro de la Agencia se creará el *Equipo Nacional de Respuesta a Incidentes de Seguridad Informática* (**"CSIRT Nacional"**), el que tendrá entre sus principales funciones responder ante ciberataques o incidentes de ciberseguridad, cuando éstos sean de efecto significativo.

Francisco de Aguirre N°3720, piso 4, Vitacura, Santiago, Chile +56 (2) 3263 76 80

Para más información, ponerse en contacto:

Jorge Lembeye
jlembeye@lembeye.cl
+56 9 8288 6928

Reginald Horn
rhorn@lembeye.cl
+56 9 8240 8924

MECANISMOS DE CONTROL, INFRACCIONES Y SANCIONES

Infracciones de los Servicios Esenciales.

Las infracciones aplicables a los Servicios Esenciales se califican en leves, graves y gravísimas.

Se destacan las siguientes infracciones *leves*:

- Entregar fuera de plazo la información que se le requiera cuando ella no fuere necesaria para la gestión de un incidente de ciberseguridad.
- Incumplir las instrucciones generales o particulares impartidas por la Agencia en los casos que no estén sancionados como infracción grave o gravísima.

Se destacan las siguientes infracciones *graves*:

- No haber implementado los protocolos y estándares establecidos por la Agencia para prevenir, reportar y resolver incidentes de ciberseguridad.
- No haber implementado los estándares particulares de ciberseguridad.

Se destacan las siguientes infracciones *gravísimas*:

- Entregar a la Agencia información manifiestamente falsa o errónea, cuando ella sea necesaria para la gestión de un incidente de ciberseguridad.
- Incumplir las instrucciones generales o particulares impartidas por la Agencia durante la gestión de un incidente de impacto significativo.

Infracciones de los Operadores de Importancia Vital.

Las infracciones aplicables a los OIV se califican en leves, graves y gravísimas.

Se destacan las siguientes infracciones *leves*:

- No comunicar al CSIRT Nacional la realización continua de operaciones de revisión, ejercicios y demás acciones que señala la ley.

Francisco de Aguirre N°3720, piso 4, Vitacura, Santiago, Chile +56 (2) 3263 76 80

Para más información, ponerse en contacto:

Jorge Lembeye
jlembeye@lembeye.cl
+56 9 8288 6928

Reginald Horn
rhorn@lembeye.cl
+56 9 8240 8924

- No contar con programas de capacitación, formación y educación continua para los trabajadores.
- No designar un delegado de ciberseguridad.

Se destacan las siguientes infracciones *graves*:

- No haber implementado el sistema de gestión de seguridad de la formación continuo conforme a lo dispuesto en la ley.
- No haber elaborado o implementado los planes de continuidad operacional y ciberseguridad conforme a lo dispuesto en la ley.

Se destacan las siguientes infracciones *gravísimas*:

- No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, cuando éste posea un impacto significativo.
- La reincidencia en una misma infracción grave dentro del período de un año.

<u>Sanciones.</u>

La infracción a los preceptos de la LMC conlleva la imposición de multas a beneficio fiscal, de acuerdo con la siguiente escala:

- Las infracciones leves serán sancionadas con multa de hasta 5.000 UTM, o hasta 10.000 UTM si se trata de un operador de importancia vital.
- Las infracciones graves serán sancionadas con multa de hasta 10.000 UTM, o hasta 20.000 UTM si se trata de un operador de importancia vital.
- Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 UTM, o hasta 40.000 UTM si se trata de un operador de importancia vital.

Las multas serán fijadas teniendo en consideración, entre otros antecedentes, las medidas necesarias para resguardar la seguridad informática de las operaciones del infractor, el grado de exposición a los riesgos, la gravedad de los efectos de los ataques y el tamaño y la capacidad económica del infractor.

Francisco de Aguirre N°3720, piso 4, Vitacura, Santiago, Chile +56 (2) 3263 76 80

ENTRADA EN VIGENCIA DE LA LMC.

La entrada en vigencia de la LMC se encontrará condicionada a la dictación de un decreto con fuerza de ley del Ministerio del Interior que deberá ser dictado en el plazo de un año contado desde la publicación de la LMC.

Este decreto determinará la fecha de iniciación de actividades por parte de la Agencia y podría establecer un periodo distinto para su implementación y operación. Se establece un plazo de 180 días para la dictación de los reglamentos que establece la ley por parte del Ministerio del Interior.

Para más información, ponerse en contacto:

Jorge Lembeye
jlembeye@lembeye.cl
+56 9 8288 6928

Reginald Horn
rhorn@lembeye.cl
+56 9 8240 8924

Francisco de Aguirre N°3720, piso 4, Vitacura, Santiago, Chile +56 (2) 3263 76 80