REPÚBLICA DE CHILE
MINISTERIO
SECRETARIA GENERAL DE LA PRESIDENCIA

FORMULA INDICACIONES AL PROYECTO DE LEY QUE ESTABLECE UNA LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN (BOLETÍN N° 14847-06)

Santiago, 26 de septiembre de 2023

N° 170-371/

A S.E. EL

PRESIDENTE

DE LA CÁMARA

DE DIPUTADAS

Y DIPUTADOS

Honorable Cámara de Diputadas y Diputados:

En uso de mis facultades constitucionales, tengo a bien poner en conocimiento de V.E. que vengo en formular las siguientes indicaciones al proyecto de ley que establece una ley marco sobre ciberseguridad e infraestructura crítica de la información, a fin de que sean consideradas durante la discusión del mismo en el seno de esta H. Corporación:

AL ARTÍCULO 4

1) Para reemplazar el artículo 4, por el siguiente:

"Artículo 4.- Ámbito de aplicación. La presente ley se aplicará a las instituciones que presten servicios calificados como esenciales según lo establecido en los incisos segundo y tercero de este artículo y a aquellas que sean calificadas como operadores de importancia vital, de conformidad con lo dispuesto en los artículos 5 y 6 de esta ley.

Son servicios esenciales aquellos provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional; los prestados bajo concesión de servicio

público; y los proveídos 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 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.

La Agencia podrá calificar otros servicios 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.

Dicha calificación deberá someterse al proceso de consulta pública y se regirá por las disposiciones de la ley N°19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.".

ARTÍCULOS 5 y 6, NUEVOS

2) Para intercalar los siguientes artículos 5 y 6, nuevos, pasando los

actuales artículos 5 y 6 a ser artículos 7 y 8, y así sucesivamente:

"Artículo 5.- Operadores de Importancia Vital. La Agencia establecerá mediante resolución dictada por el o la Directora Nacional, según se establece en el artículo siguiente, a los prestadores de servicios esenciales que sean calificados como operadores de importancia vital.

La Agencia podrá calificar como operadores de importancia vital a quienes reúnan los siguientes requisitos:

1.- que la provisión de dicho servicio dependa de las redes y sistemas informáticos; y,

2.- 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 operadores de importancia vital a instituciones privadas que, aunque no tengan la calidad de prestadores de servicios esenciales, reúnan los requisitos indicados en el inciso anterior y cuya calificación sea indispensable por haber adquirido 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.

En cualquier caso, siempre se deberá tener en consideración el tamaño de la institución privada, especialmente las características y necesidades de las micro, pequeñas y medianas empresas, tal como se definen en la ley N°20.416.

Artículo 6.- Procedimiento de calificación de los operadores de importancia vital. Al menos cada tres años, la Agencia deberá revisar y actualizar la calificación de operadores de importancia vital mediante una resolución dictada por la Directora o el Director Nacional.

Para los efectos del inciso anterior, la Agencia requerirá informe fundado a los organismos públicos con competencia sectorial para que se pronuncien sobre aquellas instituciones públicas y privadas que deban calificarse como operadores de importancia vital. Dichos informes deberán evacuarse en la forma prescrita en el artículo 37 bis de la ley N°19.880.

Recibidos los informes indicados precedentemente la Agencia dispondrá de un plazo de treinta días corridos para evacuar un informe que contendrá la nómina preliminar de las instituciones calificadas como operadores de importancia vital. Esta nómina preliminar deberá ser sometida a consulta pública por un plazo de treinta días corridos sólo respecto de las instituciones privadas, en la forma que determine el reglamento de la presente ley. Respecto de las instituciones públicas, se deberá requerir informe del Ministerio de Hacienda, en los términos del inciso precedente.

Terminado el proceso de consulta pública y recibido el informe del Ministerio de Hacienda, la Agencia dispondrá de treinta días corridos para elaborar el informe que contendrá la

nómina final de instituciones que deban ser calificadas como operadores de importancia vital, individualizándolas en la forma que señale el reglamento.

Cumplidas las etapas anteriores, la Agencia, mediante resolución fundada de su Director o Directora, determinará los operadores de importancia vital.

En contra de la resolución que se dicte sólo podrá deducirse recurso de reposición dentro del plazo de diez días corridos contado desde la respectiva notificación a que se refiere el artículo 46 de la ley N° 19.880. El recurso deberá resolverse dentro del plazo de veinte días corridos.

Un reglamento expedido por el ministerio a cargo de la seguridad pública contemplará los demás aspectos del procedimiento que sean necesarios para su correcta ejecución.".

AL ACTUAL ARTÍCULO 5, QUE HA PASADO A SER ARTÍCULO 7

3) Para reemplazar los incisos primero, segundo, tercero, cuarto, y quinto, del actual artículo 5, que ha pasado a ser artículo 7, por los siguientes:

"Las instituciones obligadas por la presente ley deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.

El cumplimiento de estas obligaciones exige la debida implementación de los protocolos y estándares establecidos por la Agencia, así como de los estándares particulares de ciberseguridad dictados de conformidad a

la regulación sectorial respectiva. El objeto de estos protocolos y estándares será la prevención y gestión de los riesgos asociados a la ciberseguridad, así como la contención y mitigación del impacto que los incidentes pueden tener sobre la continuidad operacional del servicio prestado o la confidencialidad y la integridad de la información o de las redes o sistemas informáticos de conformidad con lo prescrito en la presente ley.

Para efectos de emitir las medidas de seguridad a que se refiere el inciso primero, la Agencia deberá observar lo prescrito en el artículo 23, según corresponda. Dichos protocolos y estándares deberán someterse a consulta pública, en la misma forma y plazo señalados en el inciso tercero del artículo 6. La medida deberá publicarse junto con el informe en que se justifique el rechazo o modificación de las observaciones que correspondan.

La Agencia deberá establecer medidas de seguridad diferenciadas según el tipo de organización de que se trate, teniendo especialmente en consideración las características y posibilidades de las pequeñas y medianas empresas definidas por la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño.".

AL ACTUAL ARTÍCULO 6, QUE HA PASADO A SER ARTÍCULO 8

4) Para reemplazar el actual artículo 6, que ha pasado a ser artículo 8, por el siguiente:

"Artículo 8°. Deberes específicos de los operadores de importancia vital.

Todos los operadores de importancia vital deberán:

a) 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.

Este sistema deberá permitir evaluar tanto la probabilidad como el potencial impacto de un incidente de ciberseguridad.

b) Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de seguridad de la información, de conformidad a lo que señale el reglamento.

c) Elaborar e implementar planes de continuidad operacional y ciberseguridad, los cuales deberán certificarse en conformidad al artículo 26 de la presente ley, y deberán someterse a revisiones periódicas por parte de los sujetos obligados, con una frecuencia mínima de dos años.

Con todo, la Agencia podrá instruir a uno o más operadores de importancia vital, fundadamente y por motivos sobrevinientes graves, la certificación de sus planes de continuidad operacional o ciberseguridad en un plazo menor al indicado en el párrafo precedente; sin embargo, la Agencia sólo podrá ejercer esta facultad, respecto de cada operador de importancia vital, siempre que la certificación tenga al menos un año de vigencia.

d) 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, en la forma que determine el reglamento.

e) 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, si fuera necesario.

f) Contar con las certificaciones que señale el artículo 26 de la presente ley.

g) Informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, especialmente cuando involucren datos personales y no exista otra disposición legal que requiera su notificación; o cuando sea necesario para prevenir la ocurrencia de nuevos incidentes o para gestionar uno que ya hubiera ocurrido.

h) Contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene.

i) Designar un delegado de ciberseguridad quien actuará como contraparte de la Agencia e informará a la autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado o a los directores, gerentes, administradores o ejecutivos principales, según lo definan las instituciones privadas.".

AL ACTUAL ARTÍCULO 20, QUE HA PASADO A SER ARTÍCULO 22

5) Para modificar el actual artículo 20, que ha pasado a ser 22, en el siguiente sentido:

a) Modifícase el literal b) en el siguiente sentido:

i) Reemplázase la expresión "Sectoriales", la primera vez que aparece, por la frase "que pertenezcan a organismos de la Administración del Estado".

ii) Suprímese, la expresión "por parte de los CSIRT Sectoriales,".

iii) Agrégase, el siguiente párrafo final, nuevo:

"Cuando los ciberataques o incidentes puedan afectar el normal funcionamiento del sistema financiero, la respuesta del CSIRT Nacional deberá realizarse en coordinación con el Consejo de Estabilidad Financiera creado por la ley N° 20.789. Sin perjuicio de la obligación del CSIRT Nacional de comunicar al mencionado Consejo sobre el incidente, podrá tomar medidas sin esperar respuesta en casos de urgencia calificada.".

b) Reemplázase, en el literal d), la expresión "Sectoriales" por la frase "que pertenezcan a organismos de la Administración del Estado.".

AL TÍTULO IV

6) Para reemplazar el encabezado del título IV "Otras instituciones intervinientes" por "Coordinación regulatoria y otras disposiciones".

AL ACTUAL ARTÍCULO 21, QUE HA PASADO A SER ARTÍCULO 23

7) Para reemplazar el actual artículo 21, que ha pasado a ser artículo 23, por el siguiente:

"Artículo 23. Coordinación regulatoria. Cuando la Agencia deba dictar protocolos, estándares técnicos o

instrucciones de carácter general en el ejercicio de sus funciones, y estos tengan efectos en las áreas de competencia de otra entidad sectorial, deberá previamente remitir la información relevante a dicha entidad y solicitar un informe con el propósito de prevenir posibles conflictos normativos y garantizar la coordinación, cooperación y colaboración efectivas entre ambas autoridades.

La autoridad sectorial requerida deberá evacuar su informe dentro de un plazo de treinta días corridos a partir de la fecha en que recibió la solicitud indicada en el inciso anterior. La Agencia considerará el contenido de este informe en la motivación del acto administrativo de carácter general que emita. Transcurrido el plazo sin que se hubiere recibido el informe correspondiente, la Agencia procederá a emitir los protocolos, estándares técnicos o instrucciones generales requeridos.

Cuando una autoridad sectorial, en el ejercicio de sus atribuciones establecidas en sus leyes orgánicas, deba emitir actos administrativos de carácter general que tengan efectos en los ámbitos de competencia de la Agencia en conformidad a la presente ley, deberá remitir a la Agencia la información pertinente y solicitar un informe con el objeto de prevenir posibles conflictos normativos y garantizar la coordinación, cooperación y colaboración entre ambas entidades. Además, en el ejercicio de estas atribuciones, las autoridades sectoriales deben tener en cuenta, al menos, los protocolos, estándares técnicos e instrucciones generales previamente emitidos por la Agencia.

Lo establecido en los incisos anteriores no se aplicará en los casos en que el acto administrativo respectivo requiera una aplicación inmediata o en el

plazo más breve posible atendida a su naturaleza y urgencia, siempre que se justifique dicha circunstancia y se deje constancia. No obstante, en estos casos, la Agencia deberá, en un plazo de tres días corridos, proporcionar a las autoridades sectoriales competentes, o viceversa según corresponda, todos los documentos tenidos a la vista y solicitar un informe con el fin de cumplir con los objetivos mencionados en los incisos primero y tercero.".

AL ACTUAL ARTÍCULO 22, QUE HA PASADO A SER ARTÍCULO 24

8) Para reemplazar el actual artículo 22, que ha pasado a ser artículo 24, por el siguiente:

"Artículo 24. Normativa Sectorial. Las autoridades sectoriales podrán emitir normativas generales, técnicas e instrucciones necesarias para fortalecer la ciberseguridad en las instituciones de su sector, en conformidad con la regulación respectiva y siguiendo lo dispuesto en el artículo anterior, cuando corresponda.

Las instituciones supervisadas deberán cumplir obligatoriamente con estas normas e instrucciones en la gestión de sus riesgos, de acuerdo con la autoridad sectorial que las haya emitido. La fiscalización y sanción relacionadas con estas disposiciones se regirán por las leyes respectivas de dicha autoridad sectorial.

Cuando las normas o instrucciones emitidas por una autoridad sectorial establezcan obligaciones para un sector a fin de prevenir incidentes de ciberseguridad, que tengan, al menos, efectos equivalentes a las obligaciones previstas en los protocolos, normas o instrucciones de la Agencia, prevalecerán

las disposiciones de la autoridad sectorial. Esto no afectará los deberes de coordinación establecidos en el artículo 23 ni la aplicación de las normas de la presente ley. No obstante, si las normas o instrucciones de una autoridad sectorial no cubren a todas las entidades de un sector o solo se aplican a una parte de sus supervisados, los protocolos, normas o instrucciones de la Agencia seguirán siendo plenamente aplicables a las entidades no exceptuadas en los términos indicado en este inciso.

Para efectos de lo indicado en el inciso anterior, la Agencia y la autoridad sectorial correspondiente deberán previamente dictar una norma conjunta de carácter general. Dicha norma tendrá por objeto establecer criterios para la evaluación de la equivalencia de los efectos entre una normativa o instrucción.

Lo anterior no será aplicable a la Comisión para el Mercado Financiero, la cual deberá integrar en el correspondiente acto administrativo los antecedentes y fundamentos que permitan determinar la equivalencia de los efectos de una norma o instrucción. Esto se llevará a cabo tomando en consideración los elementos contenidos en el informe elaborado por la Agencia, de conformidad con el artículo 23.".

REPÚBLICA DE CHILE
MINISTERIO
SECRETARIA GENERAL DE LA PRESIDENCIA

Dios guarde a V.E.,

GABRIEL BORIC FONT
Presidente de la República

CAROLINA TOHÁ MORALES
Ministra del Interior
y Seguridad Pública

Ministerio de Hacienda
Dirección de Presupuestos
Reg. 209GG

I.F. N° 209/27.09.2023
I.F. N° 142/10.07.2023
I.F. N° 064/11.04.2023

I.F. N° 211/21.11.2022
I.F. N° 204/11.11.2022
I.F. N° 43/10.03.2022

Informe Financiero Complementario

Indicaciones al Proyecto de Ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información

Boletín N°14.847-06

I. Antecedentes

Mediante las presentes indicaciones (N° 170-371) se realizan modificaciones al proyecto de ley antes referido, entre las que destacan las siguientes:

- Se delimita el ámbito de aplicación de la ley a las instituciones que presten servicios calificados como esenciales y a aquellas que sean calificadas como operadores de importancia vital, incorporando una definición, calificación, y procedimiento para calificar como tal a cada una de ellas.
- Se actualizan los deberes generales de las instituciones a las que se aplica la ley en términos de medidas para prevenir, reportar y resolver incidentes de ciberseguridad, y cumplir los protocolos y estándares establecidos por la Agencia, o de aquellos dictados por la regulación sectorial según corresponda.
- En el mismo sentido, los deberes específicos establecidos por la ley son aplicables solamente a los operadores de importancia vital, obligando a estos a certificar los planes de continuidad operacional y ciberseguridad de acuerdo a lo estipulado en la ley, siendo sometidos a revisión periódica cada dos años.
- Se modifica la denominación del Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT) Sectorial, siendo reemplazada por los CSIRT que pertenezcan a organismos de la Administración del Estado.
- Se añade como función del CSIRT Nacional el responder en coordinación con el Consejo de Estabilidad Financiera (CEF) en caso de ciberataques o incidentes que puedan afectar el normal funcionamiento del sistema financiero, pudiendo actuar sin esperar respuesta en casos de urgencia calificada.
- Se establece una coordinación regulatoria entre la Agencia y las autoridades sectoriales para la dictación de protocolos y estándares técnicos o instrucciones de carácter general que tengan claros efectos en los ámbitos de competencia de la Agencia y una autoridad sectorial.
- Se suprimen las facultades especiales otorgadas a las autoridades sectoriales, sustituyéndolas por una normativa sectorial, la cual faculta a estas para dictar

normativas de carácter general o instrucciones necesarias para la ciberseguridad de su sector. En caso de una norma o instrucción cuyo objeto es prevenir incidentes de ciberseguridad, la autoridad sectorial y la Agencia deberán dictar previamente una norma de carácter general conjunta, que establezca criterios para determinar la equivalencia de los efectos de una norma o instrucción. Lo anterior no será aplicable a la Comisión para el Mercado Financiero (CMF).

II. Efecto de las indicaciones sobre el Presupuesto Fiscal

Estas indicaciones **no irrogarán mayor gasto fiscal** respecto de lo indicado en los Informes Financieros antecedentes (N°s 142, 64, de 2023 y, 43, 204 y 211, de 2022), dado que no modifican aspectos esenciales que impliquen un mayor gasto respecto de los informes financieros previos, y las obligaciones que se derivan de las mismas, serán implementadas con cargo a la dotación y presupuestos vigentes de las instituciones respectivas.

III. Fuentes de información

- Mensaje de S.E. el Presidente de la República, mediante el cual realiza indicaciones al Proyecto de Ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.

Ministerio de Hacienda
Dirección de Presupuestos
Reg. 209GG

I.F. N° 209/27.09.2023
I.F. N° 142/10.07.2023
I.F. N° 064/11.04.2023

I.F. N° 211/21.11.2022
I.F. N° 204/11.11.2022
I.F. N° 43/10.03.2022

DIRECCIÓN DE PRESUPUESTOS - DIRECTORA - Ministerio de Hacienda

JAVIERA MARTÍNEZ FARIÑA
Directora de Presupuestos

Visado Subdirección de Presupuestos:

DIRECCIÓN DE PRESUPUESTOS - SUB DIRECTORA - Ministerio de Hacienda

Visado Subdirección de Racionalización y Función Pública:

DIRECCIÓN DE PRESUPUESTOS - SUBDIRECCIÓN DE RACIONALIZACIÓN FUNCIÓN PÚBLICA - MINISTERIO DE HACIENDA