

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

Santiago, 11 de octubre de 2023

N° 184-371/

Honorable Cámara de Diputadas y Diputados:

A S.E. EL
PRESIDENTE
DE LA H.
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 ACTUAL ARTÍCULO 9 QUE HA PASADO A SER
ARTÍCULO 11

1) Para reemplazar el actual artículo 9, que ha pasado a ser artículo 11, por el siguiente:

"Artículo 11. Atribuciones. Para dar cumplimiento a su objeto, la Agencia tendrá las siguientes atribuciones:

a) Asesorar al Presidente de la República en la elaboración y aprobación de la Política Nacional de Ciberseguridad, y de los planes y programas de acción específicos para su implementación, ejecución y evaluación.

b) Dictar los protocolos y estándares que señala el artículo 7; las instrucciones



generales y particulares, de carácter obligatorio, para las instituciones, tanto públicas como privadas obligadas por la presente ley; y las demás disposiciones necesarias para la aplicación y el cumplimiento de esta ley y sus reglamentos.

c) Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias en materia de ciberseguridad; los protocolos y estándares técnicos, y las instrucciones generales y particulares que dicte al efecto.

d) Coordinar y supervisar al CSIRT Nacional y a los demás pertenecientes a la Administración del Estado; y requerir de estos la información que sea necesaria para el cumplimiento de sus fines.

e) Establecer una coordinación con el CSIRT de la Defensa Nacional, en lo relativo a los estándares y tiempos de comunicación de incidentes de ciberseguridad o vulnerabilidades, así como respecto a las materias que serán objeto de intercambio de información.

f) Crear y administrar un Registro Nacional de Incidentes de Ciberseguridad.

g) Calificar, mediante resolución fundada y en la forma prevista en los artículos 4, 5 y 6 de esta ley, a los servicios esenciales y a los operadores de importancia vital.

h) Requerir a las entidades obligadas por la presente ley que hayan visto afectados sus servicios por un incidente de ciberseguridad o ciberataque, que entreguen a los potenciales afectados información veraz, suficiente y oportuna sobre su ocurrencia, conforme lo dispuesto en el literal g) del artículo 8 de la presente ley.

i) Diseñar e implementar, en coordinación con el Ministerio de Educación,



cuando corresponda, planes y acciones de educación, formación ciudadana, investigación, innovación, entrenamiento, fomento y difusión, destinados a promover el desarrollo nacional de una cultura de ciberseguridad.

j) Requerir a los organismos de la Administración del Estado y a las instituciones privadas señaladas en el artículo 4 de la presente ley acceso a la información necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido. Especialmente, podrá requerir el acceso al registro de actividades de las redes y sistemas informáticos que permitan comprender detalles de los incidentes de seguridad que puedan haber ocurrido.

Para el ejercicio de esta atribución, la instrucción siempre tendrá carácter particular, debiendo especificarse la información solicitada y fundarse debidamente. Cuando la información referida en el inciso anterior incluya datos personales estos deberán ser anonimizados, siempre que ello no entorpezca el ejercicio de las funciones de la Agencia. En cualquier caso, los datos personales sólo podrán ser tratados dando estricto cumplimiento a lo dispuesto en la ley 19.628, y en particular, al principio de finalidad, sin perjuicio de lo que define la presente ley y sus reglamentos.

k) Requerir, mediante instrucción de su Director o Directora, en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible, el acceso a redes o sistemas informáticos. Este requerimiento deberá notificarse sin demora al requerido, debiendo éste dar las facilidades que sean necesarias.

En caso de que la Agencia requiriera la restricción del acceso o uso de redes o sistemas informáticos deberá actuar conjuntamente con la autoridad sectorial correspondiente.



l) Cooperar con organismos públicos e instituciones privadas, en materias propias de su competencia, sin perjuicio de las atribuciones de otros organismos del Estado.

La Agencia servirá de punto de contacto con las autoridades nacionales de ciberseguridad extranjeras o sus homólogos y con los organismos internacionales con competencia en materia de ciberseguridad.

Cuando se trate de la cooperación con Estados y organizaciones internacionales, dicha actividad deberá realizarse en coordinación con el Ministerio de Relaciones Exteriores, en conformidad con lo previsto en el inciso primero del artículo 2 de la ley N° 21.080.

m) Prestar, cuando sus recursos humanos, técnicos y financieros así lo permitan, asesoría técnica a los organismos del Estado e instituciones privadas afectados por un incidente de ciberseguridad que haya comprometido sus activos informáticos críticos o afectado el funcionamiento de su operación, cautelando siempre los deberes de reserva de información que esta ley le impone, así como los consagrados por la mencionada ley N°19.628.

n) Coordinar y colaborar interagencialmente con los organismos integrantes del Sistema de Inteligencia del Estado en la identificación de amenazas y la gestión de incidentes o ciberataques que puedan representar un riesgo para la seguridad nacional.

ñ) Fiscalizar el cumplimiento de las disposiciones de esta ley, sus reglamentos, protocolos, estándares técnicos y las instrucciones generales y particulares que emita la Agencia en ejercicio de las atribuciones conferidas en la ley.

Para el cumplimiento de su función fiscalizadora, la Agencia podrá realizar



inspecciones; instruir de manera particular auditorías por sí o mediante terceros autorizados y análisis de seguridad basados en criterios de evaluación de riesgos objetivos, los cuales deberán ser no discriminatorios, equitativos y transparentes. La entidad fiscalizada deberá cooperar en todo momento con los funcionarios de la Agencia o con los terceros autorizados por ella, según corresponda.

Asimismo, la Agencia podrá requerir el acceso a sistemas informáticos, datos, documentos y demás información que fuere necesaria para el desempeño de sus funciones de supervisión y fiscalización; instruir de manera particular a los sujetos obligados que realicen pruebas que demuestren la implementación de los planes de continuidad operacional y ciberseguridad, referidos en la letra c) del artículo 8 °. Adicionalmente, podrá citar a declarar, respecto de hechos cuyo conocimiento estime necesario para el cumplimiento de sus funciones, a los socios, directores, administradores, representantes, empleados, y cualquier persona que, a cualquier título, preste o haya prestado servicios para las personas o entidades fiscalizadas, así como a toda persona que hubiere ejecutado o celebrado con ellas actos o convenciones de cualquier naturaleza. No obstante, no estarán obligadas a concurrir a declarar las personas indicadas en el artículo 361 del Código de Procedimiento Civil, a las cuales la Agencia, para los fines expresados en el párrafo precedente, deberá pedir declaración por escrito.

Para el ejercicio de esta atribución podrá establecer la forma, plazos y procedimientos para que las entidades fiscalizadas cumplan la obligación de presentar los antecedentes e informaciones referidos en los párrafos precedentes.

o) Instruir el inicio de procedimientos sancionatorios y sancionar las infracciones e incumplimientos en que incurran las instituciones obligadas por la presente



ley respecto de sus disposiciones, reglamentos e instrucciones generales y particulares que emita la Agencia. Para tales efectos, y de manera fundada, podrá citar a declarar, en los términos señalados en el literal n) de este artículo, entre otros, a los representantes legales, administradores, asesores y dependientes de la institución de que se trate, así como a toda persona que haya tenido participación o conocimiento respecto de algún hecho que sea relevante para resolver el procedimiento sancionatorio. La declaración podrá tomarse presencialmente o por otros medios que aseguren su integridad y fidelidad.

p) Fomentar la investigación, innovación, capacitación y entrenamiento frente a amenazas, vulnerabilidades e incidentes de ciberseguridad y, en conjunto con los Ministerios de Economía, Fomento y Turismo, y de Ciencia, Tecnología, Conocimiento e Innovación, diseñar planes y acciones que fomenten el desarrollo o fortalecimiento de la industria de ciberseguridad local.

q) Realizar el seguimiento y evaluación de las medidas, planes y acciones elaborados en el ejercicio de sus funciones.

r) Informar al CSIRT de la Defensa Nacional y a los CSIRT de los organismos de la Administración del Estado los reportes o alarmas de incidentes de ciberseguridad y de vulnerabilidades existentes, conocidas o detectadas en su sector que considere relevantes, pudiendo sugerir determinados planes de acción.

s) Determinar, conforme al informe técnico que el CSIRT Nacional elabore para estos efectos, las categorías de incidentes o vulnerabilidades de ciberseguridad que estarán eximidas de notificación.

t) Certificar el cumplimiento de los estándares de ciberseguridad correspondientes



por parte de los organismos de la Administración del Estado.

u) Otorgar y revocar las acreditaciones correspondientes a los centros de certificación, en los casos y bajo las condiciones que establezca esta ley y el reglamento respectivo.

v) Establecer los estándares que deberán cumplir las instituciones que provean bienes o servicios al Estado, y las normas de seguridad para el desarrollo de los sistemas y programas informáticos que sean utilizados por los organismos del Estado.

w) Establecer estándares de ciberseguridad y deberes de información al público sobre riesgos de seguridad de dispositivos digitales disponibles a consumidores finales.

x) Administrar la Red de Conectividad Segura del Estado (RCSE).

y) Coordinar anualmente durante el mes de octubre, un ejercicio nacional de comprobación de capacidades de ciberseguridad, en cumplimiento de la ley N° 21.113, que declara el mes de octubre como el mes nacional de la ciberseguridad.

z) Realizar todas aquellas otras funciones que las leyes le encomienden especialmente.”.

**AL ACTUAL ARTÍCULO 34 QUE HA PASADO A SER
ARTÍCULO 36**

2) Para reemplazar el literal b) del actual artículo 34, que ha pasado a ser artículo 36, por el siguiente:

“b) La Agencia podrá iniciar un procedimiento sancionatorio, de oficio o a petición de parte, o como resultado de un proceso de fiscalización. Sin perjuicio de lo



anterior, deberá abstenerse cuando exista un procedimiento administrativo en curso, o dejar de conocer si se iniciare un procedimiento administrativo por la autoridad sectorial correspondiente dentro de los plazos legales, respecto de los mismos hechos y fundamentos jurídicos, en ejercicio de las atribuciones que correspondan a una autoridad sectorial de conformidad con lo establecido en el artículo 24.

En caso de que la Agencia tome conocimiento de un supuesto hecho infractor cuya fiscalización y sanción corresponda a una autoridad sectorial, deberá informar entregando todos los antecedentes. Transcurridos tres meses desde recibida dicha comunicación sin que la autoridad sectorial hubiere iniciado un procedimiento sancionatorio, la Agencia podrá iniciarlo, informando a la autoridad sectorial que deberá abstenerse de hacerlo.

El plazo podrá ampliarse hasta por 3 meses adicionales, a solicitud de la autoridad sectorial, en caso de que ésta informe a la Agencia del inicio de un proceso de fiscalización que pudiere resultar en un procedimiento sancionatorio. Junto con la apertura del expediente, la Agencia deberá designar un funcionario o una funcionaria responsable de la instrucción del procedimiento, que recibirá el nombre de instructor o instructora. En el evento de que producto de una denuncia se iniciare un procedimiento administrativo sancionador, el denunciante tendrá la calidad de interesado, para todos los efectos legales.”.



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. 218GG

I.F. N° 218/11.10.2023
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° 184-371) se realizan modificaciones al proyecto de ley antes referido, entre las que destacan las siguientes:

- a) En términos de información, se faculta a la Agencia para requerir a:
- i. El CSIRT Nacional y a los demás organismos pertenecientes a la Administración del Estado la información que sea necesaria para el cumplimiento de sus fines;
 - ii. Las entidades obligadas por la presente ley que hayan visto afectados sus servicios por un incidente de ciberseguridad o ciberataque, que entreguen a los potenciales afectados información veraz, suficiente y oportuna sobre su ocurrencia;
 - iii. Los organismos de la Administración del Estado y a las instituciones privadas señaladas, la información necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido;

Además, la Agencia podrá requerir, mediante instrucción de su Director o Directora, el acceso a redes o sistemas informáticos en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible. En caso de que la Agencia requiriera la restricción del acceso o uso de redes o sistemas informáticos deberá actuar conjuntamente con la autoridad sectorial correspondiente.

- b) Modificar la atribución de la Agencia para cooperar con organismos internacionales, restringiéndola a servir como punto de contacto con las autoridades nacionales de ciberseguridad extranjeras o sus homólogos, y con los organismos internacionales con competencia en materia de ciberseguridad, y cooperando con dichas organizaciones sujeta a la coordinación con el Ministerio de Relaciones Exteriores.





Ministerio de Hacienda
Dirección de Presupuestos
Reg. 218GG

I.F. N° 218/11.10.2023
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

- c) Para el cumplimiento de la función fiscalizadora de la Agencia:
- i. Se permite instruir de manera particular auditorías por sí o mediante terceros autorizados, y análisis de seguridad basados en criterios de evaluación de riesgos objetivos. Además, establece que la entidad fiscalizada deberá cooperar en todo momento con los funcionarios de la Agencia o con los terceros autorizados por ella, según corresponda.
 - ii. Facultar a esta para instruir de manera particular a los sujetos obligados que realicen pruebas que demuestren la implementación de los planes de continuidad operacional y ciberseguridad.
 - iii. Exceptuar de la obligación de concurrir a declarar respecto de hechos cuyo conocimiento estime necesario para el cumplimiento de sus funciones, a las personas indicadas en el artículo 361 del Código de Procedimiento Civil, las cuales deberán pedir declarar por escrito.
- d) Establecer estándares de ciberseguridad y deberes de información al público sobre riesgos de seguridad de dispositivos digitales disponibles a consumidores finales.
- e) Determinar que los operadores de importancia vital deben obtener las certificaciones de ciberseguridad que señala la ley y las que determine la Agencia mediante reglamento a través de organismos que sean parte del registro de entidades certificadoras autorizadas, a cargo de la Agencia. Además, la Agencia podrá homologar certificaciones técnicas internacionales o extranjeras sobre ciberseguridad mediante resolución fundada de su director o directora.
- f) Especificar que, en caso de un procedimiento sancionatorio iniciado por la Agencia, esta deberá abstenerse cuando existiera un procedimiento administrativo en curso, o dejar de conocer si se iniciare uno por la autoridad sectorial correspondiente dentro de los plazos legales. Igualmente, en caso de que la Agencia tome conocimiento de un supuesto hecho infractor cuya fiscalización y sanción corresponda a una autoridad sectorial, deberá informar entregando todos los antecedentes pudiendo iniciarlo transcurridos tres meses desde recibida dicha comunicación sin que la autoridad sectorial hubiere iniciado un procedimiento sancionatorio. El plazo podrá ampliarse hasta por 3 meses adicionales, a solicitud de la autoridad sectorial, en caso de que ésta





Ministerio de Hacienda
Dirección de Presupuestos
Reg. 218GG

I.F. N° 218/11.10.2023
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 a la Agencia del inicio de un proceso de fiscalización que pudiere resultar en un procedimiento sancionatorio.

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 209, 142, 64, de 2023 y, 43, 204 y 211, de 2022), 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. 218GG

I.F. N° 218/11.10.2023

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



J. Martínez Fariña
JAVIERA MARTINEZ FARIÑA
Directora de Presupuestos

Visado Subdirección de Presupuestos:



Visado Subdirección de Racionalización y Función Pública:

