Ley Marco de Ciberseguridad (21.663)

Cambios en la Protección Digital

Promulgación: 26-MAR-2024
Publicación: 08-ABR-2024

PREPARADO POR

Carlos Ramirez (CPP)

RESUMEN

La ley establece un **marco regulador en ciberseguridad** para organismos estatales y privados en Chile, enfocándose en la prevención y respuesta a incidentes.

Define términos clave como activo informático, ciberataque, auditorías de seguridad, y establece principios de control de daños, cooperación y seguridad en el ciberespacio.

Crea diferentes **organismos para cumplir con los objetivos** establecidos:

- **Agencia Nacional de Ciberseguridad**
- **Consejo Multisectorial de Ciberseguridad**
- **CSIRT Nacional**
- **CSIRT de la Defensa Nacional**
- **Comité Interministerial de Ciberseguridad**
- **Red de Conectividad Segura del Estado (RCSE)**

Esta ley aplica a **servicios esenciales** (de entidades públicas y privadas) comprendiendo a los provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional, los prestados bajo concesión de servicio público y los provistos por instituciones privadas que realicen actividades que puedan afectar la seguridad nacional, orden público, medioambiente o la sociedad en caso de interrupciones, y permite que la Agencia identifique otros servicios críticos.

También se aplica a los denominados **"operadores de importancia vital"** regulando el procedimiento para tal calificación; siendo necesario que la provisión de sus servicios dependa de las redes y sistemas informáticos, y que la perturbación de sus servicios tenga un impacto significativo en la seguridad y el orden público, en la provisión de servicios esenciales, y el efectivo cumplimiento de las funciones del Estado o, en general, de los servicios que éste debe proveer.

Se fijan **deberes específicos para los operadores de importancia vital**, dentro de los que se encuentran:

1. Implementar un sistema de gestión de la información continuo
2. Elaborar e implementar planes de continuidad operacional y ciberseguridad

3. Realizar continuamente operaciones de revisión, adoptar medidas oportunas y expeditas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad.
4. Aplicar de manera permanente medidas para prevenir, reportar y resolver incidentes de ciberseguridad.

La ley **declara como confidencial la información** de la Agencia y los CSIRT, estableciendo sanciones en el Código Penal para infracciones de esta confidencialidad.

La Agencia y autoridades sectoriales **supervisarán y sancionarán infracciones** según su gravedad (leves, graves y gravísimas), estableciendo un sistema sancionatorio con multas que oscilan entre 5,000 y 40,000 UTM (entre 348.000 y 2.775.000 USD).

Sin embargo, la ley **excluye de su regulación a órganos autónomos constitucionales**, como el Senado, la Cámara de Diputadas y Diputados, el Poder Judicial, Contraloría, entre otros.

Se introducen modificaciones a la ley N° 20.424, estatuto del Ministerio de Defensa Nacional y a la ley N°21.459 (delitos informáticos).

Finalmente, se señala que el Presidente de la Republica deberá dictar, en el plazo de un año contado desde su publicación, las normas necesarias para determinar, entre otras cosas, el periodo para la entrada en vigencia.

OBJETO

Establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones obligadas, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

ÁMBITO DE APLICACIÓN

Se aplicará a los servicios esenciales y a los operadores de importancia vital.

Servicios esenciales

Provistos por la Administración del Estado y el Coordinador Eléctrico Nacional; Prestados bajo concesión de servicio público; 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 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.

Operadores de importancia vital

La Agencia establecerá, a los prestadores de servicios esenciales que sean calificados como operadores de importancia vital.

Requisitos para calificar como operadores de importancia vital:

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.

OBLIGACIONES DE CIBERSEGURIDAD

Deberes Generales:

Las instituciones obligadas deberán aplicar medidas permanentes para prevenir, reportar y resolver incidentes de ciberseguridad.

Deberes específicos de los operadores de importancia vital:

1. Implementar un sistema de gestión de seguridad de la información continuo, que debe evaluar la probabilidad y potencial impacto de un incidente de ciberseguridad
2. Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión
3. Elaborar e implementar planes de continuidad operacional y ciberseguridad, que deberán certificarse y someterse a revisiones periódicas, con una frecuencia mínima de dos años.
4. 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.
5. Adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad.
6. Contar con las certificaciones establecidas por la Agencia.
7. 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; o cuando sea necesario para prevenir la ocurrencia de nuevos incidentes o para gestionar uno que ya hubiera ocurrido.
8. Contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciber higiene.
9. Designar un delegado de ciberseguridad, quien actuará como contraparte de la Agencia.

Deber de reportar.

Al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos, tan pronto les sea posible y conforme al siguiente esquema:

- **Dentro de 3 horas** contado desde que **se tiene conocimiento** de la ocurrencia del ciberataque o incidente de ciberseguridad, se deberá enviar una alerta temprana sobre la ocurrencia del evento.

- **Dentro del plazo máximo de 72 horas**, una **actualización de la información**, que incluya una evaluación inicial del incidente, su gravedad e impacto, así como indicadores de compromiso, si estuvieran disponibles.

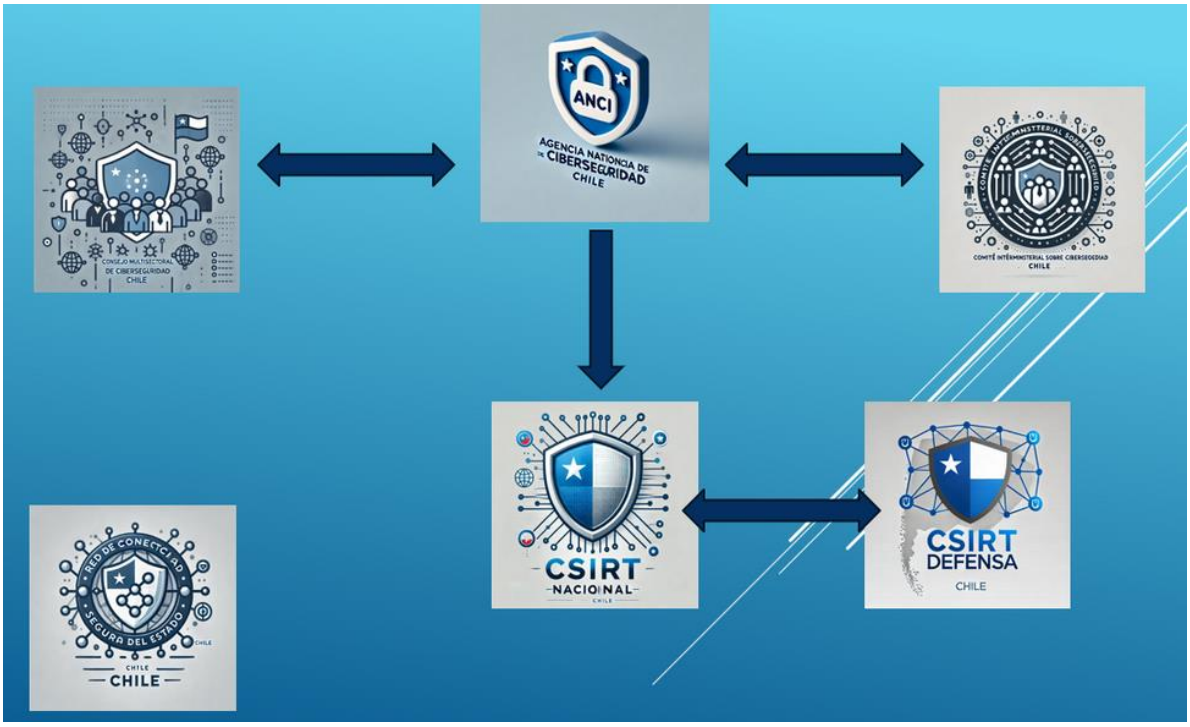
  *Si la institución afectada fuera un **operador de importancia vital** y éste viera afectada la prestación de sus servicios esenciales, la actualización de la información deberá entregarse al CSIRT Nacional en el **plazo máximo de 24 horas** contado desde el conocimiento del incidente.*

- **Dentro del plazo máximo de 15 días** corridos contado desde el envío de la alerta temprana, un informe final que al menos contenga:
  - Una descripción detallada del incidente, incluyendo su gravedad e impacto.
  - El tipo de amenaza o causa principal del incidente.
  - Las medidas de mitigación aplicadas y en curso.
  - Si procede, las repercusiones transfronterizas del incidente.

Los **operadores de importancia vital** deberán, además, informar al CSIRT Nacional su plan de acción, tan pronto lo hubieren adoptado. El plazo para la adopción de un **plan de acción** en **ningún caso podrá ser superior a 7 días** corridos desde el conocimiento de la ocurrencia del incidente.

ORGANISMOS QUE SE CREAN...

- Agencia Nacional de Ciberseguridad (ANCI)
- Consejo Multisectorial de Ciberseguridad
- Red de Conectividad Segura del Estado (RCSE)
- Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional)
- Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional (CSIRT de la Defensa Nacional)
- Comité Interministerial sobre Ciberseguridad



INFRACCIONES Y SANCIONES

La autoridad sectorial y la Agencia son competentes para fiscalizar, conocer y sancionar las infracciones, así como ejecutar las sanciones a la presente ley, sin perjuicio de la facultad de los organismos de la Administración del Estado de poner en conocimiento del organismo competente las infracciones a la norma de que tomaren conocimiento.

Infracciones.

Las infracciones a las obligaciones que se imponen a los obligados por se califican en:

- Leves
- Graves
- Gravísimas.

Infracciones leves:

1. Entregar fuera de plazo la información que se le requiera cuando ella no fuere necesaria para la gestión de un incidente de ciberseguridad
2. Incumplir las instrucciones generales o particulares impartidas por la Agencia en los casos que no estén sancionados como infracción grave o gravísima
3. Cualquier infracción a las obligaciones que la ley establece y que no tenga señalada una sanción especial

Infracciones graves:

1. No haber implementado los protocolos y estándares establecidos por la Agencia para prevenir, reportar y resolver incidentes de ciberseguridad
2. No haber implementado los estándares particulares de ciberseguridad
3. Entregar fuera de plazo la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de ciberseguridad
4. Entregar a la Agencia información manifiestamente falsa o errónea.
5. Incumplir la obligación de reportar
6. Negarse injustificadamente a cumplir una instrucción de la Agencia o entorpecer deliberadamente el ejercicio de sus atribuciones durante la gestión de un incidente

de ciberseguridad
7. La reincidencia en una misma infracción leve dentro de un año.

Infracciones gravísimas:

1. Entregar a la Agencia información manifiestamente falsa o errónea, cuando ella sea necesaria para la gestión de un incidente de ciberseguridad
2. Incumplir las instrucciones generales o particulares impartidas por la Agencia durante la gestión de un incidente de impacto significativo
3. No entregar la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de impacto significativo
4. La reincidencia en una infracción grave dentro de un año.

Infracciones de los operadores de importancia vital

Los operadores de importancia vital podrán ser sancionados por infringir las disposiciones referentes a sus deberes específicos (artículo 8º).

Las infracciones de dichas disposiciones por estos operadores se califican en leves, graves y gravísimas.

Infracciones leves:

1. No mantener el registro de las acciones de seguridad
2. No comunicar al CSIRT Nacional la realización continua de operaciones de revisión, ejercicios y demás acciones que señaladas
3. No contar con programas de capacitación, formación y educación continua para los trabajadores
4. No designar un delegado de ciberseguridad
5. No dar cumplimiento a la instrucción particular de la Agencia en orden a certificar los planes de continuidad operacional
6. No contar con las certificaciones que exija la ley

Infracciones graves:

1. No haber implementado el sistema de gestión de seguridad de la información continuo
2. No haber elaborado o implementado los planes de continuidad operacional y

ciberseguridad

3. No informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos
4. 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
5. La reincidencia en una misma infracción leve dentro del período de un año.

Infracciones gravísimas:

1. 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
2. La reincidencia en una misma infracción grave dentro del período de un año.

Sanciones.

Las infracciones a esta ley conllevan la imposición de una multa 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.

¿Qué medidas deben adoptar las Empresas?

Para implementar la Ley Marco de Ciberseguridad, las empresas deben seguir varios pasos clave que aseguren la alineación con los estándares y directrices establecidos por el gobierno.

1. Identificación: En principio partir por identificar si la Empresa presta alguno de los servicios esenciales mencionados por la Ley
2. Comprensión de la Legislación: Las empresas deben entender los requisitos de la ley, incluyendo sus principios, obligaciones, y el alcance de las normativas. Esto implica capacitar al personal clave en los aspectos fundamentales de la ley y sus implicaciones.
3. Liderazgo: se debe designar a una persona con un rol responsable en la organización, con la capacidad para liderar la implementación de las normas técnicas que exigirá la agencia, sin perder de vista las medidas y acciones legales que deberá asumir.
4. Evaluación de Riesgos: Realizar una evaluación completa de riesgos en ciberseguridad para identificar vulnerabilidades y amenazas en sus sistemas, datos y procesos. Esta evaluación debe enfocarse en los activos críticos que podrían ser objeto de ataques.
5. Diseño de una Estrategia de Ciberseguridad: Basándose en los resultados de la evaluación, las empresas deben crear una estrategia de ciberseguridad alineada con los principios de la ley, como la seguridad por diseño y la privacidad por defecto. Esta estrategia debe incluir políticas y procedimientos específicos.
6. Establecimiento de un Plan de Respuesta a Incidentes: Desarrollar un plan de respuesta a incidentes que incluya protocolos para la detección, análisis y respuesta a posibles incidentes de seguridad. La empresa debe designar un equipo de respuesta y definir procedimientos claros de comunicación y recuperación.
7. Implementación de Controles de Seguridad: Adoptar medidas técnicas y administrativas para proteger la infraestructura crítica y la información sensible. Estos controles pueden incluir sistemas de detección de intrusiones, autenticación multifactor, encriptación de datos y monitoreo continuo de la red.
8. Colaboración con el CSIRT Nacional y Otros Organismos: Mantener una

comunicación constante y colaboración con el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT) y otros organismos relevantes, informando de incidentes importantes y adoptando recomendaciones.

9. Capacitación y Concienciación: Capacitar a los empleados sobre la importancia de la ciberseguridad y la normativa aplicable, promoviendo una cultura organizacional de ciberseguridad. Esto incluye entrenamiento en buenas prácticas, como la identificación de correos electrónicos de phishing y el manejo seguro de la información.
10. Auditoría y Cumplimiento: Realizar auditorías internas regulares para evaluar el cumplimiento con la ley y la efectividad de las medidas de ciberseguridad. Las auditorías permiten identificar áreas de mejora y demostrar cumplimiento ante posibles inspecciones.
11. Actualización y Mejora Continua: Dado que las amenazas cibernéticas evolucionan constantemente, las empresas deben actualizar sus prácticas y tecnologías de seguridad regularmente, asegurando que sus sistemas estén alineados con los avances y recomendaciones del CSIRT y otros organismos de ciberseguridad.

Implementar estos pasos ayuda a las empresas no solo a cumplir con la Ley Marco de Ciberseguridad, sino también a fortalecer su capacidad de respuesta frente a incidentes y proteger su información y activos críticos de manera proactiva.