Ley Marco de Ciberseguridad de Chile

Guía de aplicación exclusiva para empresas

SEGURIDADAMÉRICA.COM
Fortaleciendo Internet

Contenidos

1. ¿Cuáles son los objetivos de la Ley?

- Establecer la institucionalidad, principios y la normativa 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 y otras instituciones vinculadas y mecanismos de control de responsabilidad frente a posibles infracciones., y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

2. ¿A qué entidades se aplica la Ley?

A organismos estatales y sociedades en que tengan participación accionaria superior al 50% o mayoría en el directorio.
La ley se aplicará a las instituciones que presten servicios calificados como esenciales, estas serán públicas o privadas según el caso. Es la ANCI la responsable de establecer y clasificar a estas entidades.

3. ¿Cuáles son los principios establecidos por Ley?

- **Principio de control de daños:** implica que al sufrir ciberataques o incidentes se adoptar medidas para evitar la escalada del ciberataque o incidente.

- **Principio de cooperación con la autoridad:** para resolver los incidentes de ciberseguridad se deberá prestar la cooperación debida con la autoridad competente y con sectores vinculados.

- **Principio de coordinación:** implica la Agencia de Ciberseguridad (ANCI) y las autoridades sectoriales deberán cumplir sus cometidos coordinadamente.

- **Principio de seguridad en el ciberespacio:** impone la obligación al Estado de resguardar la seguridad en el ciberespacio.

- **Principio de respuesta responsable:** implica que al llevar adelante métodos de respuesta a incidentes, no se deberá avanzar a la realización o apoyo de operaciones ofensivas.

- **Principio de seguridad informática:** toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias.

- **Principio de racionalidad:** las medidas para la gestión de incidentes de ciberseguridad, las obligaciones y el ejercicio de las facultades de la Agencia deberán ser necesarias y proporcionales al grado de exposición a los riesgos, y al eventual impacto social y económico.

- **Principio de seguridad y privacidad por defecto y desde el diseño:** los sistemas informáticos, aplicaciones y tecnologías de la información deben diseñarse, implementarse y gestionarse teniendo en cuenta la seguridad y la privacidad de los datos personales que procesan.

4. ¿Cuáles son los deberes a los que se someten las entidad obligadas al cumplimiento de la ley?

- Aplicar constantemente medidas para prevenir, reportar y resolver incidentes de ciberseguridad, a nivel organizacional, tecnológico y cualquier otra medida necesaria.

- Cumplir con protocolos y estándares establecidos por la Agencia, así como los estándares particulares de ciberseguridad dictados de conformidad a la regulación sectorial respectiva.
  Habrá obligaciones específicas para operadores de importancia vital como la implementación de sistemas de gestión de seguridad de la información, elaborar planes de continuidad, realizar auditorías constantes, informar incidentes sufridos, entre otros.

- Deber de reportar Todas las instituciones públicas y privadas tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos. La norma establece procedimientos y aclara situaciones.

5. ¿Qué es la ANCI y cómo funciona?

La Agencia Nacional de Ciberseguridad (ANCI) es un organismo que crea la norma que servirá de servicio público descentralizado, técnico y especializado.

Objetivos principales:

- Asesorar al Presidente de la República en materia de ciberseguridad.
- Colaborar en la protección de los intereses nacionales en el ciberespacio velando por la protección, promoción y respeto del derecho a la seguridad informática.

Atribuciones principales:

- Asesorar al Presidente de la República en la elaboración y aprobación de la Política Nacional de Ciberseguridad.
- Dictar los protocolos y estándares.
- 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.
- Coordinar y supervisar al CSIRT Nacional.
- Crear y administrar un Registro Nacional de Incidentes de Ciberseguridad.
- Diseñar e implementar planes y acciones de formación ciudadana, capacitación, fortalecimiento, difusión y promoción de la cultura en ciberseguridad.
- Cooperar con organismos públicos e instituciones privadas, en materias propias de su competencia, sin perjuicio de las atribuciones de otros organismos del Estado.

- Fiscalizar el cumplimiento de las disposiciones de la ley y reglamentos.

- 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.

- Certificar el cumplimiento de los estándares de ciberseguridad correspondientes por parte de los organismos de la Administración del Estado.

Deber de reserva de la Agencia: La Agencia deberá mantener la reserva de la información que llegue a conocer en el desempeño de sus funciones según la calidad de resguardo de la información. Deberá ejercer sus funciones teniendo en cuenta el respeto a los derechos fundamentales de las personas, particularmente el respeto y resguardo del derecho a la vida privada y del derecho a la protección de datos personales.

6. ¿Qué es el consejo multisectorial sobre ciberseguridad?

Entidad que se crea para asesorar y formular recomendaciones a la Agencia en el análisis y revisión periódica de la situación de ciberseguridad del país.

7. ¿Qué es la red de conectividad segura del Estado?

Una entidad (abreviada RCSE), para proveer servicios de interconexión y conectividad a internet a los organismos de la Administración del Estado señalados en el artículo 1° de la ley. La Agencia generara convenios de interconexión con instituciones públicas y privadas que considere necesarios para el mejor funcionamiento de la RCSE y de los servicios adicionales que preste.

8. ¿Qué es el equipo nacional de respuesta a incidentes de seguridad informática?

Se creará dentro de la Agencia Nacional de Ciberseguridad "CSIRT Nacional", cuyas funciones principales serán:

- Responder ante ciberataques o incidentes de ciberseguridad significativos.
- Coordinar a los CSIRT que pertenezcan a organismos de la Administración del Estado.
- Servir de punto de conexión entre Equipos de Respuesta a Incidentes de Seguridad Informática extranjeros o sus equivalentes para el intercambio de información de Ciberseguridad.
- Supervisar incidentes a escala nacional.
- Realizar entrenamiento, educación y capacitación en materia de ciberseguridad.
- Difundir alertas tempranas, avisos e información sobre riesgos e incidentes para la comunidad.

9. ¿Infracciones y sanciones?

Según cada sector y reglamentos aplicables, serán las infracciones y sanciones posibles. La autoridad sectorial será competente para fiscalizar, conocer y sancionar las infracciones, así como ejecutar las sanciones de acuerdo a medidas que se hubiesen dictado por dicha autoridad. Ahora bien la ANCI sancionará las infracciones, así como las ejecutará. Las infracciones se clasifican en leves, graves y gravísimas, teniendo en cuenta que incumplimiento de obligación la haya generado.

1. Las infracciones leves serán sancionadas con multa de hasta 5.000 unidades tributarias mensuales, o hasta 10.000 unidades tributarias mensuales si se trata de un operador de importancia vital.

Se considerarán infracciones leves las siguientes:

- 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.
- Cualquier infracción a las obligaciones que esta ley establece y que no tenga señalada una sanción especial.

2. Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades tributarias mensuales, o hasta 20.000 unidades tributarias mensuales si se trata de un operador de importancia vital.

Se considerarán infracciones graves las siguientes:

- 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 deciberseguridad.

- Entregar fuera de plazo la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de ciberseguridad.

- Entregar a la Agencia información manifiestamente falsa o errónea.

- Incumplir la obligación de reportar establecida en el artículo 9º.

- Negarse injustificadamente a cumplir una instrucción de la Agencia o entorpecer deliberadamente el ejercicio de las atribuciones de la Agencia durante la gestión de un incidente de ciberseguridad, siempre que la atribución no cuente con una sanción especial.

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

3. Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 unidades tributarias mensuales, o hasta 40.000 unidades tributarias mensuales si se trata de un operador de importancia vital.

Se considerarán infracciones gravísimas las siguientes:

- 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.

- No entregar la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de impacto significativo.

- La reincidencia en una infracción grave dentro de un año.

10. Escalas de infracciones

En relación a la ley de Ciberseguridad se establecerán reglamentos para cuestiones específicas tratadas por esta y cuya finalidad es la de complementar y abordar esas cuestiones en detalle.

- **Reglamento sobre Reportes de Incidentes de Ciberseguridad:** establecerá en forma detallada y clara los procesos y procedimientos para las notificaciones de incidentes de ciberseguridad que realicen los proveedores de servicios esenciales y de importancia vital, los que por ley se encuentran obligados a hacerlo frente al CSIRT Nacional proporcionando información detallada sobre el incidente.

- **Reglamento sobre Calificación de Operadores de Importancia Vital**: el cual determinará el procedimiento para la calificación de operadores de importancia vital. El reglamento detallará las diferentes etapas del proceso, como la identificación de operadores potenciales, evaluación de la criticidad de los servicios que presen, análisis de ciberseguridad, clasificación como tal, entre otras cuestiones vinculadas.

SEGURIDADAMÉRICA.COM
Fortaleciendo Internet

Para conocer más información acerca de
Ley Marco de Ciberseguridad de Chile
visita www.ley21663.cl