Ley N°21.663 Marco de Ciberseguridad

María de los Ángeles Villanueva L.
Agencia Nacional de Ciberseguridad

LEY MARCO DE CIBERSEGURIDAD

- Disposiciones Generales (definiciones y principios)
- Disposiciones Especiales (SE y OIV)
- Regímenes Especializados (Defensa y órganos autónomos constitucionales)

LEY MARCO DE CIBERSEGURIDAD

Modelo de Gobernanza

Agencia Nacional de Ciberseguridad (ANCI)

- Consejo multisectorial y Comité Interministerial
- Red de Conectividad Segura del Estado
- CSIRT Nacional y CSIRT de Defensa Nacional

LEY MARCO DE CIBERSEGURIDAD

Modelo de Gobernanza

Agencia Nacional de Ciberseguridad (ANCI)

- Consejo multisectorial y Comité Interministerial
- Red de Conectividad Segura del Estado
- CSIRT Nacional y CSIRT de Defensa Nacional

Regular
Fiscalizar
Sancionar

LEY MARCO DE CIBERSEGURIDAD

Obligaciones

Deberes generales

- Deber de reportar
- Obligaciones especiales OIV

- Prevenir
- Reportar
- Resolver Incidentes de Ciberseguridad

LEY MARCO DE CIBERSEGURIDAD

Infracciones y sanciones

Leves
Graves
Gravísimas

LEY MARCO DE CIBERSEGURIDAD: Principios inspiradores

- Control de daños
- Cooperación con la autoridad
- Coordinación
- Seguridad en el Ciberespacio
- Respuesta responsable
- Seguridad informática
- Racionalidad
- Seguridad y privacidad por defecto y desde el diseño

LEY MARCO DE CIBERSEGURIDAD

Organismo rector de la ciberseguridad del país

Gestionar incidentes

Coordinación interinstitucional

Función normativa técnica

ULTIMA RATIO: Fiscalizadora y sancionatoria

LEY MARCO DE CIBERSEGURIDAD

- Instituciones que presten **Servicios calificados como Esenciales (SE) Inc. 2° Art. 4**
  - ✓ Provistos por los OAE (Órganos de la Administración del Estado) y por el Coordinador Eléctrico Nacional;
  - ✓ Prestados bajo concesión de servicio público;
  - ✓ Instituciones privadas que realicen las actividades señaladas. (Catálogo)

- Instituciones calificadas como **Operadores de Importancia Vital (OIV) Art. 5**
  - ✓ Mediante Resolución del Director o Directora de la ANCI

LEY MARCO DE CIBERSEGURIDAD

Deberes generales (art. 7) aplicables a todas las instituciones obligadas por la ley:

Deber de reportar (art. 9) todas las instituciones obligadas

ARTÍCULO 4°: ÁMBITO DE APLICACIÓN










ARTÍCULOS 4°: ÁMBITO DE APLICACIÓN










Calificar otros servicios como esenciales

Proceso de consulta pública

ARTÍCULOS 4°: ÁMBITO DE APLICACIÓN









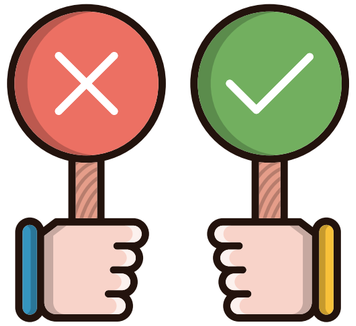

Establece los **criterios para la determinación de los Operadores de Importancia Vital** y se **faculta a la Agencia para calificarlos,** bajo ciertas condiciones, a **otras instituciones privadas** aun cuando no tengan la calidad de prestadores de servicios esenciales.

ARTÍCULO 5°: OPERADORES DE IMPORTANCIA VITAL

La ANCI establecerá mediante <u>resolución</u> dictada por el Director a los prestadores de Servicios Esenciales **que sean calificados como OIV.**

- **Provisión de dicho servicio dependa de las redes y sistemas informáticos; y**

- **Afectación, interceptación, interrupción o destrucción de sus servicios tenga un impacto significativo.**



ARTÍCULO 6°: PROCEDIMIENTO CALIFICATORIO OIV

Al menos cada 3 años ANCI deberá revisar y actualizar la calificación.

Informe fundado a los organismos públicos con competencia sectorial.

ANCI tendrá 30 días corridos para evacuar un informe con la nómina preliminar. 30 días corridos informe con nómina final. Resolución fundada.

En contra de la resolución podrán deducirse aquellos recursos a que se refiere la Ley N°19.880. (E.A.)

OBLIGACIONES SE Y OIV

PREVENIR

REPORTAR

RESOLVER INCIDENTES

MEDIDAS PERMANENTES

Implementar protocolos y estándares establecidos por la ANCI + estándares particulares dictados de conformidad a la regulación sectorial respectiva.

OBLIGACIONES SE Y OIV

Todas las instituciones señaladas en **art. 4° (S.E.)** están obligadas a:

- Reportar al CSIRT
- Tan pronto les sea posible y
- Conforme al esquema del art. 9.

DEBER GENERAL DEL ART. 7

PROTOCOLOS Y ESTÁNDARES

- Prevención y gestión de los riesgos
- Contención y mitigación del impacto (continuidad operacional, confidencialidad e integridad)
- Se deberán someter a consulta pública

DEBER GENERAL DEL ART. 7

La Agencia deberá establecer medidas de seguridad diferenciadas según el tipo de organización de que se trate.

RESPONSABLE DE VULNERABILIDADES Y EXIMENTES

Artículo 19. Notificación responsable de vulnerabilidades

La Agencia deberá mantener en secreto la notificación, sus antecedentes y la identidad de quien la realice.

Artículo 55. n°1.... sobre delitos informáticos

No será objeto de sanción penal quienes cumplan las condiciones descritas.

DEBER DE RESERVA

ARTÍCULO 55 LMC

1. *Que se encuentre inscrito en el registro que al efecto lleve la Agencia Nacional de Ciberseguridad.*

2. *Que el acceso se haya realizado habiendo informado previamente de ello a la Agencia.*

3. *Que el acceso y las vulnerabilidades de seguridad detectadas hayan sido reportadas al responsable del sistema informático y a la Agencia, tan pronto se hubiere realizado.*

4. *Que el acceso no haya sido realizado con el ánimo de apoderarse o de usar la información contenida en el sistema informático, ni con intención fraudulenta. Tampoco podrá haber actuado más allá de lo que era necesario para comprobar la existencia de una vulnerabilidad, ni habrá utilizado métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, exfiltración o destrucción de datos.*

5. *Que no haya divulgado públicamente la información relativa a la potencial vulnerabilidad.*

6. *Que se trate de un acceso a un sistema informático de los organismos de la Administración del Estado. En el resto de los casos, requerirá del consentimiento del responsable del sistema informático.*

7. *Que haya dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la Agencia.*

TÍTULO VII. INFRACCIONES Y SANCIONES

Artículo 37. Competencia de la autoridad sectorial

Artículo 38. Infracciones
Artículo 39. De las infracciones de los operadores de importancia vital.
Artículo 40. De las sanciones.

Artículo 41. Procedimiento simplificado.
Artículo 42. Procedimiento administrativo sancionador
Artículo 43. De los recursos.

Artículo 44. Forma de pago de las multas
Artículo 45. Pronto pago.

Artículo 46. Procedimiento de reclamación judicial
Artículo 47. Responsabilidad administrativa del jefe superior del OAE

ARTÍCULO 37. COMPETENCIA AUTORIDAD SECTORIAL (PREMINENCIA)

- La **autoridad sectorial** será competente para **fiscalizar, conocer y sancionar las infracciones**, así como **ejecutar las sanciones…**

- Las sanciones y procedimientos sancionatorios serán los que correspondan a la autoridad sectorial **de conformidad a su normativa**.

- Fuera de dichos casos, corresponderá a la **Agencia** fiscalizar, conocer y sancionar las infracciones así como ejecutar las sanciones a la presente ley…

ARTÍCULO 38. INFRACCIONES

LEVES
(hasta **5.000 UTM**
o hasta **10.000 UTM** para **OIV**)

Entregar **fuera de plazo** la información que se le requiera (no necesaria para la gestión de un incidente).

Incumplir instrucciones generales o particulares de la Agencia (cuando no esté sancionado como grave o gravísima).

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

ARTÍCULO 39. INFRACCIONES OIV

LEVES
(hasta **5.000 UTM**
o hasta **10.000 UTM** para **OIV**)

- No mantener el **registro de las acciones** de seguridad.
- **No comunicar al CSIRT Nacional** la realización continua de operaciones de revisión, ejercicios y demás acciones.
- No contar con **programas de capacitación,** formación y educación continua para los trabajadores.
- No **designar** un delegado de ciberseguridad, entre otras.

ARTÍCULO 38. INFRACCIONES

GRAVES
(hasta **10.000 UTM o** hasta **20.000 UTM para OIV)**

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

Entregar **fuera de plazo** la información que se le requiera (cuando fuere necesaria para la gestión de un incidente).

Incumplir la obligación de reportar.

No haber implementado los estándares particulares de ciberseguridad, entre otros.

ARTÍCULO 38. INFRACCIONES

GRAVES
(hasta **10.000 UTM o** hasta **20.000 UTM para OIV)**

Entregar a la Agencia información manifiestamente **falsa o errónea.**

Negarse injustificadamente a cumplir una instrucción o entorpecer el ejercicio de las atribuciones de la Agencia durante la gestión de un incidente de ciberseguridad, entre otras.

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

ARTÍCULO 39. INFRACCIONES

GRAVES
(hasta **10.000 UTM o** hasta **20.000 UTM para OIV)**

- No haber implementado el **sistema de gestión de seguridad** de la información contínuo.
- No haber **elaborado o implementado los planes de continuidad operacional** y ciberseguridad.
- **No informar** a los potenciales afectados sobre la ocurrencia de incidentes o ciberataque que pidiera comprometerlos.
- No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente.

ARTÍCULO 38. INFRACCIONES

GRAVÍSIMAS
(hasta **20.000 UTM o** hasta **40.000 UTM para OIV)**

Entregar **información falsa o errónea** cuando sea necesaria para la gestión de un incidente de ciberseguridad.

Incumplir las instrucciones impartidas por la Agencia durante la gestión de un incidente de impacto significativo.

La reincidencia en una infracción grave dentro de un año.

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

ARTÍCULO 39. INFRACCIONES

GRAVÍSIMAS
(hasta **20.000 UTM o** hasta **40.000 UTM para OIV)**

- No adoptar de forma oportuna las **medidas necesarias para reducir el impacto** y la propagación de un incidente de ciberseguridad de impacto significativo.

- **La reincidencia** en una misma infracción grave dentro del período de un año.

¡Gracias!

María de los Ángeles Villanueva L.
Agencia Nacional de Ciberseguridad