

Noviembre 2024



Ley Marco de Ciberseguridad en Chile

¿Qué implica?



Contenidos

¿Qué es y por qué es tan importante la ciberseguridad?	2
Objetivos de la ley	4
Definiciones	5
Nuevas entidades	8
Alcance	10
¿Cómo saber si una empresa califica como prestadora de servicios esenciales?	10
El rol de los Operadores de Importancia Vital	11
Obligaciones	13
Deberes a cumplir	13
Reportes	15
Infracciones y sanciones	16
Competencia de la autoridad sectorial	16
Clasificación de infracciones	16
Prepara tu empresa	18
Acciones importantes que las autoridades implicadas deben tomar	18
Medidas de seguridad que puedes aplicar	20

¿Qué es y por qué es tan importante la **ciberseguridad**?

La ciberseguridad es la preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.

Este término se aplica en diferentes contextos, desde los negocios hasta la informática móvil.

En la actualidad, la ciberseguridad es crucial para garantizar el ejercicio pleno de los derechos individuales, ya que disponer de un entorno digital seguro posibilita el ejercicio de éstos en las relaciones personales, laborales, con el Estado y privados.



En el último tiempo ha habido un aumento y mayor sofisticación en los delitos digitales y ciberataques, los que han afectado las cadenas de suministro, infraestructura crítica, pública, privada y universidades. Por esta razón, los países están desarrollando nuevas legislaciones, políticas y medidas que permitan lidiar con estas nuevas formas de criminalidad.

Con la publicación en el Diario Oficial de la Ley N°21.663 Marco de Ciberseguridad, ésta se convierte en el modelo de gobernanza en ciberseguridad en Chile, representando un avance importante en materia de seguridad digital para todos los ciudadanos.



Objetivos de la ley

La Ley Marco de Ciberseguridad en Chile se enfoca en crear entidades y un modelo de gobernanza que promuevan la implementación de estándares para mejorar la prevención, contención, resolución y respuesta a ciberataques.



Establecer una nueva institucionalidad que permita estructurar, regular y coordinar las acciones de ciberseguridad de las organizaciones privadas y públicas que prestan servicios esenciales para el funcionamiento del país.



Establecer los requisitos mínimos para la prevención, contención, resolución y respuesta frente a los incidentes de ciberseguridad que se generen.



Establecer las atribuciones y obligaciones tanto de los órganos del Estado como de las instituciones privadas que posean infraestructura crítica de la información, estableciendo mecanismos de control y un sistema de infracciones y sanciones.



Instaurar una cultura pública en materia de seguridad digital que ayude a formar a los ciudadanos y empresas frente al creciente número de amenazas digitales.



Proteger la información y los derechos digitales en materia de integridad, confidencialidad, disponibilidad, privacidad y protección de datos personales.

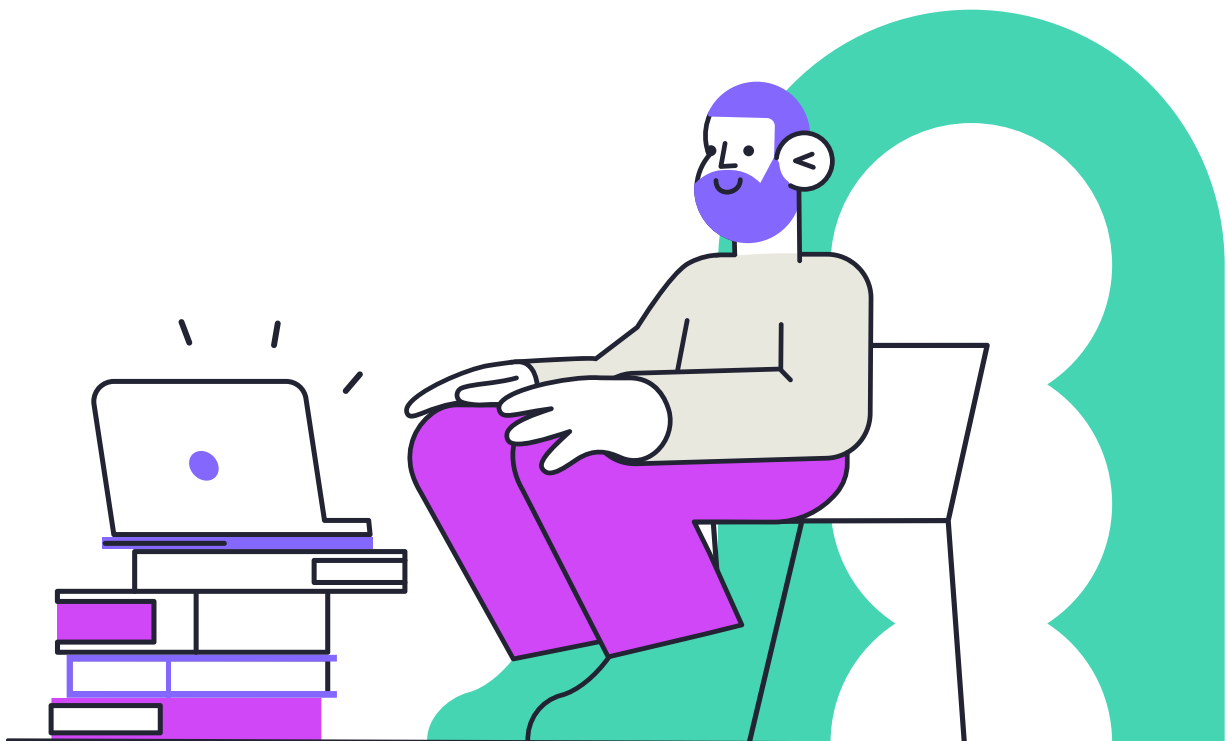


Fortalecer las capacidades para prevenir, detectar y dar respuesta a incidentes de ciberseguridad.

Definiciones

Para efectos de esta ley, existen ciertas definiciones que serán de utilidad para su comprensión y manejo:

- » **Activo informático:** toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.
- » **Auditorías de seguridad:** procesos de control destinados a revisar el cumplimiento de las políticas y procedimientos que se derivan del Sistema de Gestión de la Seguridad de la Información (SGSI).
- » **Autenticación:** proceso que da cuenta del origen legítimo de la información.
- » **Ciberataque:** intento de destruir, exponer, alterar, deshabilitar, extraer u obtener acceso o hacer uso no autorizado de un activo informático.



- » **Confidencialidad:** garantía de que la información será protegida para que no sea divulgada sin consentimiento, o entregada a individuos, entidades o procesos no autorizados.
- » **Incidente de ciberseguridad:** todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.
- » **Integridad:** propiedad que consiste en garantizar la exactitud de los datos, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.
- » **Red y sistema informático:** conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.



- » **Resiliencia:** capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado. Asimismo, se incluye la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.
- » **Riesgo:** posibilidad de que ocurra un incidente de ciberseguridad. La magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias del mismo.
- » **Sistema de Gestión de la Seguridad de la Información (SGSI):** conjunto de políticas y procedimientos para la administración eficiente de la accesibilidad de la información en una empresa u organización. El término SGSI es muy utilizado por la ISO/IEC 27001.
- » **Vulnerabilidad:** debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.



Nuevas entidades

A partir de la Ley Marco de Ciberseguridad, se crean las siguientes entidades:

- ✓ **Agencia Nacional de Ciberseguridad (ANCI):** esta agencia consiste en un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, de carácter técnico y especializado.

Su objetivo es asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, velar por la protección, promoción y respeto del derecho a la seguridad informática, y coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

- ✓ **Equipo de Respuesta ante Incidentes de Seguridad Informática de la Defensa Nacional (CSIRT):** se trata del organismo encargado de coordinar, proteger y asegurar las redes y sistemas del Ministerio de Defensa Nacional, así como los servicios esenciales y operadores vitales para la defensa nacional.

Además de crear un CSIRT Nacional, **se habilita la creación de CSIRT sectoriales.**



- ✓ **Consejo multisectorial:** se crea un consejo que tiene carácter consultivo, cuya función será asesorar y hacer recomendaciones a la ANCI en el análisis y revisión periódica del estado de la ciberseguridad del país.

Adicionalmente, se encargará de analizar las amenazas actuales y potenciales relacionadas con la ciberseguridad y proponer medidas para hacerles frente.

- ✓ **Red de conectividad segura del estado:** esta nueva red ofrecerá servicios de interconexión y conectividad a internet a los organismos de la Administración del Estado como los Ministerios, las Delegaciones Presidenciales Regionales y Provinciales, las Fuerzas Armadas y la Seguridad Pública.














Alcance

La Ley Marco de Ciberseguridad aplica a instituciones del sector público y privado que califiquen como prestadores de servicios esenciales, así como aquellas que adicionalmente sean calificadas como Operadores de Importancia Vital (OIV) por la Agencia Nacional de Ciberseguridad (ANCI).

¿Cómo saber si una empresa califica como prestadora de servicios esenciales?

Los servicios esenciales son todos aquellos que proveen los organismos de la Administración del Estado o instituciones privadas, que son básicos para el normal funcionamiento del país, incluyendo todas aquellas empresas que se encarguen de:

-  Generación, transmisión y distribución de electricidad
-  Atención en salud
-  Administración de prestaciones de seguridad social
-  Suministro de agua potable y saneamiento
-  Transporte terrestre, ferroviario, aéreo o marítimo
-  Transporte, almacenamiento o distribución de combustibles
-  Banca y servicios financieros
-  Telecomunicaciones
-  Infraestructura digital y servicios digitales
-  Servicios de tecnología de la información gestionados por terceros
-  Servicios postales y de mensajería

La Agencia Nacional de Ciberseguridad tiene la capacidad de calificar otros servicios como esenciales si el rol del servicio otorgado por la empresa causa daños graves a la población, las actividades económicas, el medio ambiente, la defensa nacional y el orden público.

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

El rol de los Operadores de Importancia Vital

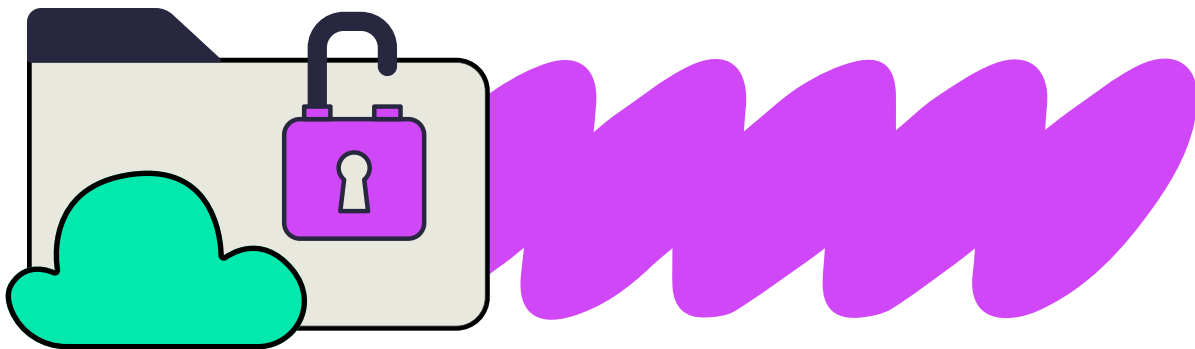
Los OIV son todos aquellos prestadores de servicios esenciales que cumplan con los siguientes requisitos:

- El servicio que ofrecen depende de redes y sistemas informáticos.
- La interrupción del servicio que prestan tiene un impacto significativo en 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.



De la misma forma en que la Agencia Nacional de Ciberseguridad puede calificar otros servicios como esenciales, también podrá calificar como Operadores de Importancia Vital a instituciones del sector privado que, aunque no tengan la calidad de prestadores de servicios esenciales, reúnen las características indicadas anteriormente así como también determinados requisitos.

Estos requisitos comprenden, el ser indispensables por haber adquirido un rol crítico en el abastecimiento de la población, la distribución o producción de bienes 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.



Al menos cada tres años la Agencia Nacional de Ciberseguridad deberá revisar y actualizar la calificación de Operadores de Importancia Vital mediante una resolución dictada por el Director o la Directora Nacional.

Para esto, la Agencia Nacional de Ciberseguridad requerirá un 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.

Obligaciones









Deberes a cumplir

Entre las obligaciones que contempla la ley, por un lado, están los **deberes generales**, que aplican tanto a prestadores de Servicios Esenciales como aquellos considerados Operadores de Importancia Vital.

- » Reportar al Equipo de Respuesta ante Incidentes de Seguridad Informática de la Defensa Nacional (CSIRT) de los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos de la ley.
- » Aplicar permanentemente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad, lo que exige la implementación de los protocolos y estándares establecidos por la Agencia Nacional de Ciberseguridad, y la regulación sectorial respectiva.



En el caso de los **Operadores de Importancia Vital**, sus deberes específicos son:

-  Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) continuo, capaz de determinar la probabilidad y el impacto de un incidente de ciberseguridad, así como mantener un registro de las acciones que componen al SGSI.
-  Crear e implementar planes de continuidad operacional que deban certificarse y realizar revisiones, como mínimo, cada 2 años.
-  Realizar operaciones de revisión de forma continua, incluyendo pruebas de penetración para la detección temprana de situaciones que comprometan la seguridad.
-  Tomar de forma oportuna acciones que reduzcan el impacto y la propagación de un incidente de ciberseguridad.
-  Contar con las certificaciones nacionales e internacionales en materia de ciberseguridad.
-  Notificar a los potenciales afectados sobre la incidencia de ciberataques que podrían afectar su información como el acceso a redes y sistemas informáticos, en especial aquellos que involucren sus datos personales.
-  Contar con programas de capacitación para sus trabajadores de forma continua.
-  Designar un delegado de ciberseguridad interno o subcontratado, encargado de informar a la autoridad competente (según sea el caso) sobre eventualidades en materia de ciberseguridad.

Reportes

Con relación a las obligaciones, tanto de prestadores de Servicios Esenciales como Operadores de Importancia Vital, se encuentra también el deber de reportar ciberataques o incidentes de ciberseguridad al CSIRT Nacional sobre cualquier evento que pueda tener un impacto significativo.

Este reporte considera:

Acción	Temporalidad
Alerta de conocimiento del incidente o ciberataque.	Dentro de las primeras 3 horas.
Evaluación inicial del incidente indicando su gravedad, impacto e indicadores.	Máximo 72 horas y 24 horas para instituciones de servicios esenciales.
Informe final con detalles del incidente, las causas, las medidas de mitigación, y las repercusiones transfronterizas, en el caso que corresponda.	Dentro de 15 días desde la alerta temprana.
Plan de acción (solo Operadores de Importancia Vital).	En un máximo de 7 días tras conocer el incidente.

Si el incidente sigue en curso, deben enviar informes de actualización hasta su resolución.

En el caso de los organismos del Estado, deben exigir a sus proveedores de servicios de TI que compartan información sobre vulnerabilidades e incidentes que puedan afectar sus redes y sistemas, con el fin de prevenir o detectar dichos incidentes.

Los contratos con estos proveedores no podrán incluir cláusulas que no permitan o limiten comunicar información sobre amenazas al respecto.

Infracciones y sanciones

Competencia de la autoridad sectorial

La autoridad sectorial tendrá la autoridad para fiscalizar, conocer y sancionar las infracciones conforme a su normativa.

En el caso de no ser la autoridad sectorial quien que cumpla esta función, la Agencia Nacional de Ciberseguridad (ANCI) será quien dará a conocer y sancionar las infracciones.

Clasificación de infracciones

Se consideran diversas sanciones por el incumplimiento de las disposiciones de la ley, las que se clasifican en 3 categorías: leves, graves y gravísimas.

<p>Leves</p>	<ul style="list-style-type: none"> • Entregar información requerida fuera de plazo • Incumplir las instrucciones generales impartidas por la ANCI • Cualquier infracción a las obligaciones sin una sanción especial que esta ley establece.
<p>Graves</p>	<ul style="list-style-type: none"> • No implementar protocolos y estándares establecidos • No reportar información o entregar ésta fuera de plazo, falsa o errónea • Negarse injustificadamente a cumplir una instrucción de la ANCI • Entorpecer deliberadamente el ejercicio de la ANCI • Reincidencia en una misma infracción leve dentro de un año.
<p>Gravísimas</p>	<ul style="list-style-type: none"> • Entregar información necesaria para la gestión de un incidente que sea falsa o errónea • Incumplir instrucciones impartidas por la ANCI o no entregar información ante un incidente de impacto significativo • Reincidencia en una infracción grave dentro de un año.

Se contemplan además infracciones y sanciones específicas ante la inobservancia de los deberes específicos de los Operadores de Importancia Vital (OIV), las que pueden ser encontradas en detalle en el Artículo 39 de la Ley 21.663.

En cuanto a las sanciones que contempla la ley, éstas se traducen en la imposición de una multa a beneficio fiscal:

Infracciones leves	Multa de hasta 5.000 UTM
Infracciones graves	Multa de hasta 10.000 UTM
Infracciones gravísimas	Multa de hasta 20.000 UTM

En el caso de los OIV, estas multas pueden incluso duplicarse.



Prepara tu empresa

Ante esta nueva política nacional de ciberseguridad, las empresas deben adaptarse para dar cumplimiento a las nuevas normativas. A continuación, te entregamos un resumen de acciones y consejos para esto.

Acciones importantes que las instituciones implicadas deben tomar









- » **Define un delegado**, con independencia de las unidades de tecnología y finanzas, que cumpla un rol que sea capaz de ejecutar e impulsar iniciativas de prevención y gestión de ciberseguridad dentro de la empresa
- » **Comprende** los aspectos que abarca la ley y sus implicancias. También debes estar en conocimiento de las normativas de seguridad aplicables de acuerdo al rubro de tu empresa, ya que, dependiendo de la industria a la que pertenezcas, existen estándares de seguridad específicos.



- » **Realiza** un análisis de brechas con otras empresas para medir el cumplimiento de normativas e implementar cambios.
- » **Construye protocolos y políticas** de seguridad informática alineados con los requerimientos de la ley.
- » **Establece un plan de acción** para que la empresa esté preparada y tenga definida una estrategia para responder ante un incidente, saber a quién acudir y qué hacer.
- » **Educa** a los trabajadores para que comprendan el ámbito de aplicación de la ley. Puedes crear instancias de capacitación y concientización, las que deben incluir el conocimiento de las políticas internas y buenas prácticas de seguridad.
- » Considera dentro del plan de capacitación y concientización, la **evaluación periódica** de la conciencia de seguridad de los trabajadores y la actualización de la información. Para esto puedes realizar charlas, pruebas de phishing, participación en seminarios, pertenecer a grupos de seguridad, entre otras.



Medidas de seguridad que puedes aplicar

-  Uso responsable de herramientas tecnológicas y redes sociales.
-  Uso de una contraseña robusta y distinta para cada sistema. Recuerda que, si eres cliente de Talana, puedes robustecer tu política de contraseña solicitándolo a través de soporte.
-  Utilizar protección anti malware.
-  No utilizar Wifi públicas para realizar transacciones económicas (compras, banca, etc) o realizar trámites personales.
-  Estar atentos para no caer en correos de phishing.
-  Navegar por sitios confiables.
-  Mantener los programas actualizados y licenciados.
-  Notificar situaciones de seguridad y/o privacidad al delegado correspondiente de tu empresa.

Mantenerse actualizados y compartir información se vuelve crucial al vivir en una sociedad en que las amenazas de ciberseguridad evolucionan día a día.