CUATRECASAS

Ley Marco de Ciberseguridad: entrada en vigencia de artículos diferidos

El 1 de marzo de 2025 comenzó a regir, en su totalidad, la Ley Marco de Ciberseguridad No. 21.663 (la "Ley")

Chile | Legal Flash | marzo 2025

ASPECTOS CLAVE:

El 1 de marzo de 2025, entraron en vigencia disposiciones relevantes de la Ley, tales como:

- La regulación sobre calificación de los Operadores de Importancia Vital ("**OIV**") y sus deberes específicos.
- El deber de reportar ciberataques e incidentes de ciberseguridad.
- El régimen de sanciones e infracciones.

La Ley representa un avance en la protección y consolidación de un entorno digital más seguro en Chile, proporcionando las bases legales para una gestión efectiva de la ciberseguridad. Sin embargo, su implementación plantea un reto importante para las instituciones y empresas, ya que su efectividad requiere de un trabajo coordinado y sostenido entre los diferentes actores involucrados.

Entrada en Vigencia

Si bien con fecha 8 de abril de 2024, se publicó en el Diario Oficial la Ley No. 21.663, Ley Marco de Ciberseguridad, la vigencia de sus disposiciones estaba supeditada a la emisión de un Decreto con Fuerza de Ley. En este sentido, con fecha 24 de diciembre de 2024, se publicó en el Diario Oficial el Decreto con Fuerza de Ley No. 1-21-663, que definió el 1 de enero de 2025 como la fecha de entrada en vigencia de la Ley y de inicio de actividades de la nueva Agencia Nacional de Ciberseguridad (la "**ANCI**").

Dicho DFL, también determinó que, con fecha 1 de marzo de 2025, entrarían en vigencia las siguientes disposiciones:

- **La calificación de los OIV.**
- **Los deberes específicos de los OIV.**
- **La obligación de reportar al Equipo de Respuesta ante Incidencias de Seguridad Informáticas ("CSIRT" por sus siglas en inglés) Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos.**
- **La regulación y régimen de infracciones y sanciones.**

Es importante recordar que la Ley crea un marco de gobernanza de la ciberseguridad. Hasta su entrada en vigencia, los asuntos de ciberseguridad en Chile se habían regulado principalmente de manera sectorial, por lo que esta Ley, junto con la Política Nacional de Ciberseguridad, marcan un hito importante y convierten a Chile en el primer país de América Latina y el Caribe en contar con una Agencia Nacional de Ciberseguridad y un marco regulatorio de vanguardia en esta materia.

La Ley conlleva la implementación de cambios relevantes en materia de ciberseguridad, lo que incluye una serie de efectos y consecuencias, tanto para el sector público como para el privado. En los siguientes párrafos identificaremos, las principales consideraciones respecto a esta nueva regulación con respecto al sector privado.

Ámbito de Aplicación

El objetivo principal de la Ley es establecer los principios y lineamientos para la prevención, detección, respuesta y gestión de incidentes y ataques cibernéticos que puedan afectar tanto al sector público como al privado.

En el ámbito privado, la Ley se aplicará a las instituciones (i) que presten servicios clasificados como "esenciales" y (ii) a las clasificadas como Operadores de Importancia Vital.

Se consideran Servicios Esenciales:

(i) Aquellos prestados por organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional;
(ii) Aquellos prestados bajo concesión de servicio público, y
(iii) Aquellos prestados por instituciones privadas que realicen las siguientes actividades:

- generación, transmisión o distribución de electricidad;
- 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 respectiva infraestructura;
- servicios bancarios, financieros y medios de pago;
- administración de prestaciones de beneficios de seguridad social (incluye AFP, AFC, Isapres, Mutualidad de Empleadores);
- servicios postales y de mensajería; y
- atención institucional de salud prestada por entidades como hospitales, clínicas, consultorios y centros médicos, y la producción y/o investigación de productos farmacéuticos.

La ANCI podrá clasificar otros servicios como Servicios Esenciales cuando su interrupción pueda causar un daño grave a (i) la vida o integridad física de la población o su suministro, (ii) a sectores relevantes de actividades económicas, (iii) al medio ambiente, (iv) al funcionamiento normal de la sociedad y/o (v) la Administración del Estado, a la defensa nacional, o a la seguridad y orden público.

Se consideran Operadores de Importancia Vital: aquellos proveedores de Servicios Esenciales que sean calificados como tales por la ANCI considerando el cumplimiento de los siguientes requisitos: (i) la prestación de su servicio depende de redes y sistemas informáticos, y (ii) 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.

Adicionalmente, la ANCI podrá calificar como OIV a instituciones privadas que, aunque no tengan la condición de proveedores de Servicios Esenciales, cumplan con los requisitos indicados en los números (i) y (ii) anteriores, y cuya calificación sea indispensable debido a (a) haber adquirido un rol crítico en el abastecimiento de la población, la distribución de bienes, o la producción de aquellos indispensables o estratégicos para el país; o (b) debido al grado de exposición de la entidad a los riesgos y la probabilidad de incidentes de ciberseguridad, incluyendo su gravedad y las consecuencias sociales y económicas asociadas.

Deberes Generales

Las entidades obligadas por la Ley deben aplicar permanentemente medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas pueden ser de naturaleza tecnológica, organizacional, física o informativa.

El cumplimiento de estas obligaciones requiere la implementación adecuada de los protocolos y estándares establecidos por la ANCI, así como los estándares específicos de ciberseguridad dictados de acuerdo con la respectiva regulación sectorial. El propósito de estos protocolos y estándares deberá ser la prevención y gestión de riesgos asociados con la ciberseguridad, así como la contención y mitigación del impacto que los incidentes puedan tener en la continuidad operacional del servicio prestado o la confidencialidad e integridad de la información o de las redes o sistemas informáticos.

Deberes Específicos para Operadores de Importancia Vital

Todas las entidades clasificadas como OIV por la ANCI deben, entre otros:

- **Implementar** un sistema continuo de gestión de seguridad de la información con el fin de determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operativa del servicio.
- **Desarrollar e implementar** planes de continuidad operacional y ciberseguridad, los cuales deben ser certificados y estar sujetos a revisiones periódicas por los sujetos obligados.
- **Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis** de redes, sistemas informáticos y sistemas para detectar acciones o programas informáticos que comprometan la ciberseguridad y comunicar la información relacionada con estas acciones o programas al CSIRT Nacional.
- Obtener una **certificación de ciberseguridad.**
- **Informar a las partes potencialmente afectadas, en la medida en que puedan ser identificadas y cuando lo requiera la ANCI,** sobre la ocurrencia de incidentes o ciberataques que puedan comprometer gravemente su información o redes y sistemas informáticos, especialmente cuando involucren datos personales y no exista otra disposición legal que requiera su notificación; o cuando sea necesario para prevenir la ocurrencia de nuevos incidentes o gestionar uno que ya haya ocurrido.
- Tener **programas de capacitación y educación** continua para sus trabajadores y colaboradores.
- Designar un **delegado de ciberseguridad.**

Deber de Reportar

Las entidades que presten Servicios Esenciales y los OIV tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos, tan pronto como sea posible, considerando un período máximo de tres horas desde el momento en que se conoce la ocurrencia del ciberataque o incidente de ciberseguridad. Adicionalmente, la regulación prevé un esquema de reportes continuos que deben emitirse dentro de los plazos y con la información solicitada en la Ley como en el Reglamento de Reporte de Incidentes de Ciberseguridad (ver más). Adicionalmente, la ANCI aprobó y publicó una taxonomía de incidentes de ciberseguridad (ver más).

La ANCI emitirá las instrucciones necesarias para la correcta creación y recepción de los reportes. En caso de obligación de notificar a más de una autoridad, la ANCI, junto con las autoridades involucradas, buscará proporcionar a las partes obligadas un sistema de ventanilla única que les permita notificar simultáneamente. Por el momento, la ANCI ha puesto a disposición de los usuarios, el sitio: https://portal.anci.gob.cl/

Se considerará que un incidente de ciberseguridad tiene un efecto significativo si puede interrumpir la continuidad de un Servicio Esencial o afectar la integridad física o la salud de las personas, así como en el caso de afectar sistemas informáticos que contengan datos personales.

Para determinar la importancia de los efectos de un incidente, se tendrán especialmente en cuenta los siguientes criterios:

- El número de personas afectadas.
- La duración del incidente.
- La extensión geográfica en relación con el área afectada por el incidente.

Agencia Nacional de Ciberseguridad

La ANCI tendrá varias facultades para cumplir con su propósito y el cumplimiento de las disposiciones de la Ley y sus regulaciones, y los protocolos, estándares técnicos e instrucciones generales y específicas que emita la ANCI en el ejercicio de las facultades que le confiere la Ley.

Para cumplir con su función de supervisión, la ANCI podrá realizar inspecciones e instruir auditorías específicas, ya sea por sí misma o a través de terceros autorizados, y análisis de seguridad basados en criterios objetivos de evaluación de riesgos.

Adicionalmente, y entre las demás facultades establecidas por la Ley, la ANCI podrá instruir el inicio de procedimientos sancionadores y sancionar las infracciones e incumplimientos cometidos por las entidades obligadas.

Cuando la ANCI o una autoridad sectorial deban emitir protocolos, estándares técnicos o instrucciones generales en el ejercicio de sus funciones, las entidades deberán prevenir posibles conflictos regulatorios, y ambas deben asegurar una coordinación, cooperación y colaboración efectiva.

Cuando las normas o instrucciones emitidas por una autoridad sectorial establezcan obligaciones para un sector a fin de prevenir incidentes de ciberseguridad, que tengan al menos efectos equivalentes a las obligaciones previstas en los protocolos, normas o instrucciones de la ANCI, prevalecerán las disposiciones de la autoridad sectorial.

Sin embargo, si las normas o instrucciones de una autoridad sectorial no cubren a todas las entidades de un sector o solo se aplican a una parte de sus entidades supervisadas, los protocolos, normas o instrucciones de la ANCI seguirán siendo plenamente aplicables a las entidades no exentas.

Infracciones y Sanciones

La autoridad sectorial será competente para supervisar, investigar y sancionar las infracciones, así como ejecutar las sanciones establecidas por las regulaciones de ciberseguridad que haya emitido y cuyos efectos sean al menos equivalentes a los de las regulaciones emitidas por la ANCI. Para este propósito, las sanciones y procedimientos sancionadores serán los correspondientes a la autoridad sectorial de acuerdo con sus regulaciones. Fuera de estos casos, será responsabilidad de la ANCI fiscalizar, conocer y sancionar las infracciones, así como ejecutar las sanciones incluidas en la Ley.

A continuación, incluimos un par de ejemplos de los comportamientos que la Ley considerará punibles:

- **Infracciones Leves:** multas de hasta 5.000 UTM o 10.000 UTM si involucra a un OIV.

  a) Presentar fuera de plazo la información requerida cuando no es necesaria para la gestión de un incidente de ciberseguridad.

b) No cumplir con las instrucciones generales o específicas emitidas por la ANCI en los casos que dicho incumplimiento no sea sancionado como infracción grave o gravísima.

c) Cualquier violación de las obligaciones establecidas en la Ley que no tenga una sanción específica.

Adicionalmente, constituirá una infracción leve para los OIV, entre otros: (i) no mantener el registro de acciones de seguridad, (ii) no informar al CSIRT Nacional sobre la realización continua de operaciones de revisión, ejercicios y otras acciones, (iii) no tener programas de capacitación, formación y educación continua, (iv) no designar un delegado de ciberseguridad, (v) no cumplir con la instrucción específica de la ANCI de certificar los planes de continuidad operacional, y (vi) no tener las certificaciones requeridas por la Ley.

- **Infracciones Graves:** multas de hasta 10.000 UTM o 20.000 UTM si involucra a un OIV.

  a) No implementar los protocolos y estándares establecidos por la ANCI para prevenir, reportar y resolver incidentes de ciberseguridad.

  b) No implementar estándares específicos de ciberseguridad.

  c) Presentar la información requerida fuera de plazo cuando es necesaria para la gestión de un incidente de ciberseguridad.

  d) Proporcionar a la ANCI información manifiestamente falsa o errónea.

  e) No cumplir con la obligación de reportar incidentes de ciberseguridad.

  f) Negarse injustificadamente a cumplir con una instrucción de la ANCI o entorpecer deliberadamente el ejercicio de las facultades de la ANCI durante la gestión de un incidente de ciberseguridad.

  g) Repetir la misma infracción leve dentro del plazo de un año.

  Adicionalmente, constituirá una infracción grave para los OIV, entre otros: (i) no haber implementado el sistema de gestión de seguridad de la información continuo, (ii) no haber elaborado o implementado los planes de continuidad operacional y ciberseguridad, (iii) no informar a las partes potencialmente afectadas sobre la ocurrencia de incidentes o ciberataques que puedan comprometer gravemente su información o redes y sistemas informáticos, cuando corresponda, (iv) no adoptar de forma oportunidad y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o ciberataque, y (v) repetir la misma infracción leve dentro del plazo de un año.

- **Infracciones Gravísimas:** multas de hasta 20.000 UTM o 40.000 UTM si involucra a un OIV.

  a) Proporcionar a la ANCI información manifiestamente falsa o errónea cuando es necesaria para la gestión de un incidente de ciberseguridad.

  b) No cumplir con las instrucciones generales o específicas emitidas por la ANCI durante la gestión de un incidente de impacto significativo.

  c) No proporcionar la información requerida cuando es necesaria para la gestión de un incidente de impacto significativo.

  d) Repetir una infracción grave dentro del plazo de un año.

Adicionalmente, constituirá una infracción gravísima para los OIV, entre otros: (i) no adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o ciberataque, cuando tenga un impacto significativo, y (ii) repetir la misma infracción grave dentro del plazo de un año.

Al fijar la multa, se considerará (i) el grado en que el infractor tomó las medidas necesarias para salvaguardar la seguridad informática de las operaciones, (ii) la probabilidad de ocurrencia del incidente, (iii) el grado de exposición del infractor a los riesgos, (iv) la gravedad de los efectos de los ataques, incluyendo sus repercusiones sociales o económicas, (v) la repetición de la infracción dentro de un período de tres años desde que ocurrió el incidente, y (vi) el tamaño y la capacidad económica del infractor.

Cuando por los mismos hechos y fundamentos legales el infractor pudiera ser sancionado bajo la Ley y bajo una o más leyes diferentes, se impondrá la sanción más grave. En ningún caso se podrán aplicar dos o más sanciones administrativas al infractor por los mismos hechos y fundamentos jurídicos.

Las infracciones previstas en la Ley estarán sujetas a un plazo de prescripción de tres años desde que se hayan cometido, período que se interrumpirá con la notificación de la presentación de cargos por los hechos constitutivos de la infracción.

Próximos Pasos

En este contexto, aún queda un largo camino por recorrer tanto para las instituciones de los 35 sectores definidos como prestadores de Servicios Esenciales por la Ley, para los futuros OIV y la ANCI, por encontrarse pendiente la emisión de normas, instrucciones, directrices e interpretaciones que no solo clarifiquen el contenido de la Ley, sino que también orienten al sector privado en su implementación. El Director Nacional de la ANCI ha subrayado que, para el 2025, se han establecido tres prioridades fundamentales que marcarán el trabajo del organismo: (i) la puesta en marcha de la ANCI, (ii) la implementación del proceso de notificación de incidentes y (iii) el primer proceso de calificación de los OIV. En este sentido, se ha reconocido la importancia de la colaboración con los gremios de los sectores regulados durante el año 2025 para la implementación efectiva de la Ley, destacando la relevancia del diálogo continuo con todos los actores involucrados; esto incluye a los reguladores sectoriales, con quienes se deberá mantener una coordinación regulatoria adecuada. La colaboración y el diálogo constante entre todas las partes interesadas serán fundamentales para asegurar una implementación efectiva y eficiente de la Ley. Además, se subraya la necesidad de establecer mecanismos claros y transparentes que faciliten la comunicación y el intercambio de información entre los diferentes sectores y la ANCI, garantizando así respuestas oportunas y coordinadas.

Contactos:

Josefina Yávar
+5622 889 9900
josefina.yavar@cuatrecasas.com

Isidora Opazo
+5622 889 9900
isidora.opazo@cuatrecasas.com

Para obtener información adicional sobre el contenido de este documento puede enviar un mensaje a nuestro equipo del Área de Conocimiento e Innovación o dirigirse a su contacto habitual en Cuatrecasas.