Cariola Díez Pérez-Cotapos

ALERTA LEGAL

Alerta Legal: Ley Marco de Ciberseguridad. Inicio del proceso de calificación de OIVs y obligación de inscripción en plataforma de reportes

05.06.2025

Carolina Flisfisch
Socia

Eduardo Vilches
Asociado Senior

José Pablo Lapostol
Asociado

Alerta Legal: Ley Marco de Ciberseguridad. Inicio del proceso de calificación de OIVs y obligación de inscripción en plataforma de reportes

Ayer miércoles 04 de junio se publicaron disposiciones claves para avanzar en la implementación de la Ley N° 21.663, Marco de Ciberseguridad (LMC). La Resolución Exenta N° 024 de la Agencia Nacional de Ciberseguridad (ANCI) inicia el primer proceso formal de calificación de Operadores de Importancia Vital (OIV), con un cronograma en dos etapas para evaluar a los Prestadores de Servicios Esenciales (PSE) según su sector económico. Además, se publicó, la Instrucción General N° 1 que regula la inscripción en la plataforma de reportes de incidentes significativos y que aplica a todos los sujetos actualmente obligados por la LMC.

A. Inicio primer procedimiento de calificación de OIV

- **Desde el 30 de mayo de 2025:** el proceso de designación de OIVs iniciará con la evaluación de los PSE que se desenvuelven en alguno de estos sectores: **i.** electricidad (generación, transmisión, distribución), **ii.** telecomunicaciones, **iii.** infraestructura digital y servicios TI gestionados por terceros, **iv.** banca, servicios financieros y medios de pago, **v.** prestadores institucionales de salud, **vi.** empresas públicas creadas por ley y **vii.** organismos de la Administración del Estado.

- **Desde el 30 de noviembre de 2025:** se evaluarán los PSE que correspondan a los sectores: **i.** transporte y distribución de combustibles, **ii.** agua potable y saneamiento, **iii.** transporte terrestre, aéreo, ferroviario o marítimo, **iv.** concesionarios de servicios públicos, **v.** seguridad social, **vi.** servicios postales y de mensajería, y **vii.** industria farmacéutica (producción/investigación).

Para calificar a un PSE como OIV la ANCI considerará los siguientes criterios:

- Que la provisión del servicio dependa de redes y sistemas informáticos.

- Que la afectación, interceptación, interrupción o destrucción de sus servicios tenga un **impacto significativo** en: a) La seguridad y el orden público, b) la provisión continua y regular de servicios Esenciales, c) el efectivo cumplimiento de las funciones del Estado, y d) en general, en los servicios que el Estado debe proveer o garantizar.

Procedimiento de calificación de OIVs

I. Inicio

- La ANCI requerirá un informe técnico a los organismos públicos competentes en el sector donde se desenvuelva el PSE, quienes deberán responder en 30 días corridos.

- Con base en dichos informes, no vinculantes, la ANCI publicará una nómina preliminar de OIVs, la que además deberá ser notificada a cada organización considerada en la referida nómina.

II. Consulta pública

- La nómina preliminar de instituciones privadas consideras OIVs se someterá a consulta pública.

- Cualquier persona natural o jurídica podrá presentar observaciones a través de la plataforma electrónica de la ANCI en un plazo de 30 días corridos.

- Tras analizar las observaciones, la ANCI publicará un resumen ejecutivo con su respuesta y, posteriormente, la nómina final de instituciones calificadas como OIV.

III. Publicación y recursos

- La nómina final se publicará en el Diario Oficial.

- Contra esta resolución pueden deducirse recursos administrativos generales, sin perjuicio de la reclamación judicial establecida en el art. 46 de la LMC.

IV. Reclamación judicial (art. 46 LMC)

- Puede interponerse ante Corte de Apelaciones de Santiago o la Corte del domicilio del reclamante.
- Debe presentarse dentro de los 15 días hábiles siguientes a la notificación de la designación como OIV.
- La Corte requerirá un informe a la Agencia y podrá abrir un término de prueba.
- Si la Corte acoge el reclamo, podrá ordenar la rectificación del acto, modificar la resolución impugnada o dejarla sin efecto.
- Finalmente, es posible recurrir ante la Ex. Corte Suprema dentro del plazo de 10 días hábiles de la decisión de la Corte de Apelaciones.

V. Efectos de la declaración de OIV

Ser OIV implica asumir obligaciones más exigentes que las aplicables a un PSE. Así, los PSE están obligados a aplicar de manera permanente las medidas para prevenir y resolver incidentes de ciberseguridad indicadas por la ANCI (pendientes de publicación), y reportar ciberataques e incidentes con efectos significativos que sufran. Mientras que un OIV, adicionalmente, debe cumplir con las siguientes obligaciones:

- Implementar un sistema de gestión de seguridad de la información.
- Desarrollar e implementar planes de continuidad operativa y ciberseguridad, los cuales deberán certificarse de conformidad con el art. 28 LMC (reglamento de ANCI aún pendiente).
- Realizar operaciones de revisión, ejercicios y análisis de redes y sistemas informáticos que comprometan la ciberseguridad, y comunicar los resultados al CSIRT Nacional.
- Tomar las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad.
- Obtener las certificaciones de ciberseguridad previstas por la ley (reglamento de ANCI aún pendiente).
- Informar a los potenciales afectados, en la medida en que puedan identificarse y cuando así lo requiera la Agencia, sobre la ocurrencia de incidentes que pudieran comprometer gravemente su información o sus redes y sistemas informáticos, especialmente cuando involucren datos personales y no exista otra disposición legal que requiera su notificación.
- Contar con programas de capacitación, educación y educación continua para sus trabajadores y colaboradores, incluyendo campañas de ciberhigiene.
- Designar un delegado de ciberseguridad, quien actuará como contraparte de la Agencia e informará a la alta dirección.

Finalmente, las sanciones a los OIV son el doble que las de los PSE: la máxima sanción a PSEs puede llegar a 20.000 UTM (app. USD 1.450.000), mientras que para OIVs puede ser de 40.000 UTM (app. USD 2.900.000).

B. Inscripción en la plataforma de reportes de incidentes significativos

Esta Instrucción complementa el art. 27° de la LMC, por el cual todos los sujetos obligados deben reportar incidentes al CSIRT Nacional y registrarse previamente en la plataforma de la ANCI.

- La inscripción debe hacerse en https://portal.anci.gob.cl por un encargado designado, quien debe tener formación o experiencia en ciberseguridad, pudiendo registrarse más de una persona por institución (titular y subrogantes).
- Para ello es obligatorio proporcionar un correo electrónico institucional, registrarse mediante uso de Clave Única, generar una contraseña robusta y contar con autenticación de dos factores (2FA).
- El nombramiento del encargado debe acreditarse mediante un documento suscrito con firma electrónica avanzada por el representante legal de la institución.

Entrada en vigencia: El 11 de junio de 2025.

Sanciones por incumplimiento: Al ser una Instrucción su incumplimiento es considerado infracción leve de la LMC y, por tanto, conlleva multa de 5000 UTM (app USD 362.500).

Plazo de cumplimiento: No especificado en la Instrucción.