# Alerta Legal

BOFILL MIR ABOGADOS

## Entra en vigencia la obligación de reportar incidentes de ciberseguridad

El día 1 de marzo de 2025 entró en vigencia la obligación de reportar ciberataques e incidentes de ciberseguridad de impacto significativo, conforme a la Ley N° 21.663, Marco de Ciberseguridad.


**Jorge Tisné**
Abogado senior
PI, Datos y Tecnología

**Roberto Natho**
Asociado
PI, Datos y Tecnología

**Martín Ramos**
Asociado
PI, Datos y Tecnología

Santiago, 13 de marzo de 2025

**El día 1 de marzo de 2025 entró en vigencia el artículo 9 de la Ley 21.663 Marco de Ciberseguridad ("Ley") respecto a la obligación de reportar incidentes de ciberseguridad.**

**El mismo día se publicaron el Decreto N°295/2024, que aprueba el Reglamento de Reporte de Incidentes de Ciberseguridad (en adelante "el Reglamento de Reporte") y la Resolución Exenta N° 7 que aprueba Taxonomía de Incidentes de Ciberseguridad ("Reglamento de Taxonomía de los Incidentes").**

Los principales elementos para tener en consideración son:

- Deber de reporte: Todas las organizaciones calificadas como **servicios esenciales y operadores de importancia vital** (en adelante "OIV") deberán reportar: (i) ciberataques; y (ii) los incidentes de ciberseguridad con efectos significativos.

- Sujetos obligados: Son obligados al deber de reporte los **Servicios Esenciales** y los **OIV**. Dentro de los Servicios Esenciales se incluyen instituciones privadas que realizan actividades definidas por la Ley Marco de Ciberseguridad.

- Incidentes que deben reportarse: Cualquier **ciberataque o incidente de ciberseguridad con efectos significativos.** Tanto ciberataque como incidente de ciberseguridad se definen en el artículo 2 de la Ley.

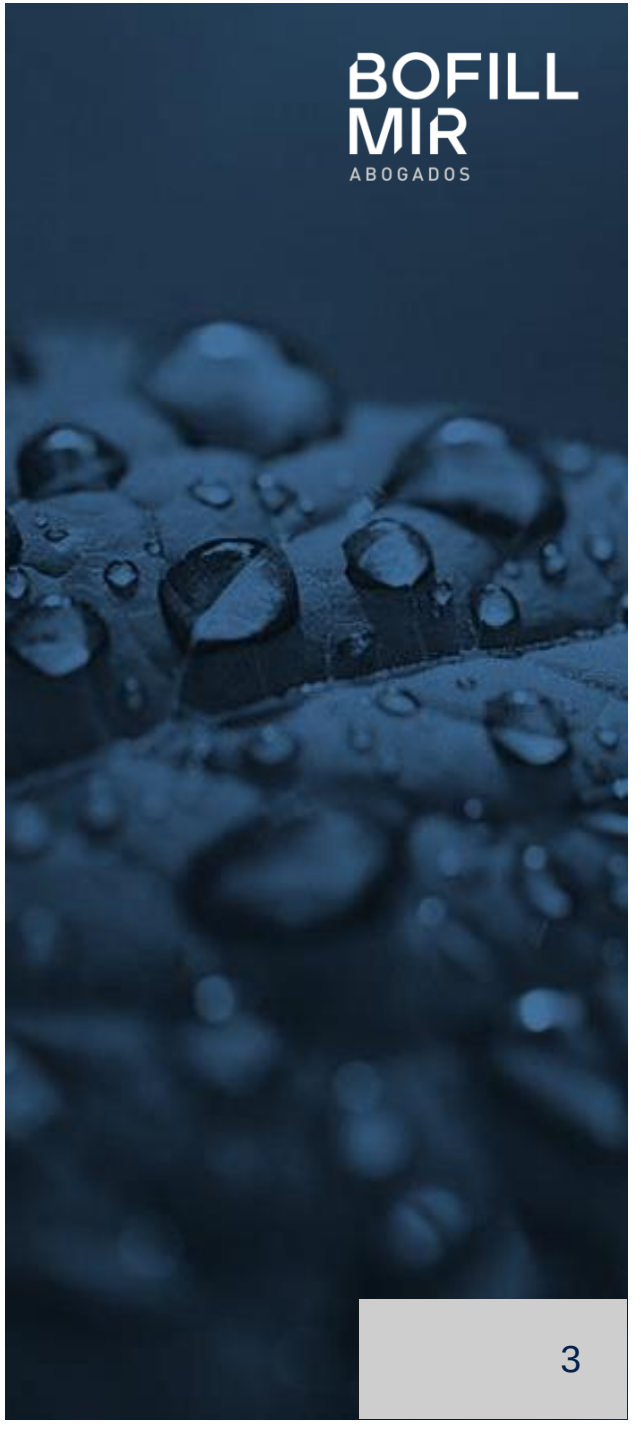
    - Ciberataque: intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.

    - 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.

- Incidente de ciberseguridad con efectos significativos: Se considera que **un incidente de ciberseguridad tiene efectos significativos si**:
  - Interrumpe un servicio esencial.
  - Afecta la integridad física o salud de las personas.
  - Compromete la confidencialidad o disponibilidad de archivos informáticos.
  - Implica un acceso no autorizado a redes o sistemas.
  - Involucra sistemas con datos personales.

- A quién debe reportarse: Los incidentes deberán ser informados al **Equipo Nacional de Respuesta a Incidentes de Seguridad Informática ("CSIRT Nacional")**, un organismo de la ANCI encargado de coordinar y gestionar la respuesta a estos eventos.

- Procedimiento y plazos de reporte: Las entidades afectadas deberán seguir un procedimiento de tres pasos:
  - Alerta temprana: Los reportes deberán realizarse en un plazo máximo de 3 horas desde que se tome conocimiento del incidente.
  - Segunda notificación: Segundo reporte de actualización de la información en un plazo máximo de 72 horas. Este plazo será de 24 horas en caso de tratarse de un OIV que haya visto afectada la prestación de sus servicios esenciales a causa del incidente.
  - Plan de acción para los OIV: Informar dentro de los 7 días posteriores desde que se tome conocimiento del incidente un plan de acción frente al incidente.
  - Informe final: Deberá enviarse dentro de un plazo máximo de 15 días corridos a partir del envío de la alerta temprana, siempre que el incidente haya sido gestionado. Si la gestión del incidente aún no se ha completado, se deberán presentar informes parciales hasta su resolución.



- Contenido mínimo de los reportes: Los reportes deberán seguir los contenidos establecidos en el Reglamento de Reporte, incluyendo, entre otros:
  - Datos para la identificación de la institución afectada.
  - Individualización y datos de contacto del encargado de ciberseguridad.
  - La fecha y hora a la que se tomó conocimiento del incidente.
  - Evidencia del ciberataque o incidente.
  - Potenciales repercusiones en otras instituciones.
  - Indicios de la ocurrencia del incidente.

- Taxonomía del incidente: Los informes deberán incluir una descripción del incidente, clasificándolo según sus efectos observables independientemente de cual pueda ser su causa u origen. Para establecer un criterio uniforme de clasificación, la ANCI estableció en el Reglamento de Taxonomía de los Incidentes las áreas de impacto y los efectos observables del incidente para ser incluidos en el reporte.

- Canales de reporte: Para realizar el reporte, la ANCI ha habilitado un canal específico a través del portal portal.anci.gob.cl, donde las instituciones deben registrarse utilizando la ClaveÚnica del funcionario encargado. Adicionalmente, en caso de contingencia, se encuentran disponibles los siguientes canales de contacto: el teléfono 1510 y el correo electrónico ayuda@anci.gob.cl.

- Sanción: El incumplimiento en la obligación de reporte conlleva una infracción grave a la Ley, la cual esta sancionada con multa de hasta 10.000 UTM (USD 700,000 aprox.) en el caso de Servicios Esenciales y de hasta 20.000 UTM (USD 1,4 millones aprox.) en el caso de OIV.

**Esta alerta legal fue preparada por el equipo de Propiedad Intelectual, Datos y Tecnología de Bofill Mir Abogados con fines informativos generales y no debe ser considerada como asesoría legal.**

En caso de preguntas o comentarios respecto de esta información, puedes comunicarte con nuestro equipo:


**Jorge Tisné**
**Abogado senior**
PI, Datos y Tecnología

**Roberto Natho**
**Asociado**
PI, Datos y Tecnología

**Martín Ramos**
**Asociado**
PI, Datos y Tecnología

Tel. +56 2 2757 7600
www.bofillmir.cl

Av. Andrés Bello 2711, piso 8,
Las Condes | Santiago, Chile