H · D
LEGAL

HDGROUP.CL

# Alerta Legal

**Protección de Datos Personales, Ciberseguridad y Nuevas Tecnologías**

**Marzo 2025**

## PUBLICACIÓN DEL REGLAMENTO DE REPORTE DE INCIDENTES ACORDE A LA LEY N° 21.663, MARCO DE CIBERSEGURIDAD Y RESOLUCIÓN N°7, DE LA AGENCIA NACIONAL DE CIBERSEGURIDAD.

+56 2 2405 3200
AV. VITACURA 2939 – 8TH FLOOR
LAS CONDES, SANTIAGO, CHILE

El pasado 1º de marzo del 2025, acorde al DFL Nº 1 (2024), de la Ley Nº 21.663 - que dio por iniciadas las actividades de la Agencia Nacional de Ciberseguridad (ANCI) el 1º de enero del 2025- entraron en vigencia las disposiciones relativas a los deberes específicos de los operadores de importancia vital, el reporte de incidentes de impacto significativo y, el régimen infraccional de la Ley Marco de Ciberseguridad.

Acorde a ello, se publicaron con misma fecha, el Decreto Nº 295/2024, que aprueba el Reglamento de Reporte de Incidentes de Ciberseguridad de la Ley, que detalla la obligación contenida en el artículo 9º de la Ley, en relación con los incidentes de impacto significativo descritos en el artículo 27º de la mencionada normativa. Este deber abarca a las instituciones públicas y privadas que prestan servicios esenciales como los operadores que hubiesen sido calificados como de importancia vital, sólo aquellos ciberataques e incidentes de ciberseguridad que pueden tener efectos significativos, ya sea porque (a) interrumpe la continuidad de un servicio esencial; (b) afecta la integridad física o la salud de las personas; (c) afecta la integridad o confidencialidad de activos informáticos o la disponibilidad de alguna red o sistema informático; (d) permite la utilización o ingreso sin autorización de redes o sistemas informáticos; (e) afecta sistemas informáticos que contengan datos personales. En ese sentido, importante es recordar que las instituciones deben reportar mediante una alerta temprana (dentro de las 3 horas), un segundo reporte (dentro de 72 horas para servicios esenciales y, 24 horas en el caso de los operadores de importancia vital), y un informe final (dentro de máximo 15 días desde

el primer reporte) para cumplir con la obligación. Su incumplimiento o retardo, puede conllevar aquellas infracciones contenidas en el Título VII.

En el mismo sentido, se publicó la Resolución Exenta Nº 7, del 2025 de la ANCI, que aprueba la taxonomía de incidentes de ciberseguridad. Esta resolución establece la plataforma dispuesta por la ANCI para que se realicen los reportes del artículo 9º de la Ley, en relación, al artículo 5º del Decreto señalado más arriba; el reporte debe contener una descripción del incidente, y la resolución nos indica que la taxonomía a utilizar acorde a los efectos observables, son: (a) impacto en el uso legítimo de recursos; (b) impacto en la confidencialidad de la información; (c) impacto en la disponibilidad de un servicio esencial; (d) impacto en la integridad de la información. Considerando el efecto del evento de seguridad, las categorías de incidentes pueden ser (i) uso no autorizado de redes y sistemas informáticos; (ii) actividades de phishing o fraude en infraestructura propia; (iii) actividades de phishing o fraude relacionadas con la institución; (iv) ejecución no autorizada de código; (v) exfiltración y/o exposición de datos; (vi) exfiltración y/o exposición de configuraciones; (vii) exfiltración y/o exposición de código fuente; (viii) indisponibilidad y/o denegación de servicios; (ix) degradación de servicios; (x) modificación no autorizada de datos, y (xi) manipulación no autorizada de configuración. Por ende, si reúne los requisitos señalados en el Decreto Nº 295, y puede ser un incidente que sea clasificado como de impacto significativo, siendo de aquellos eventos de seguridad que deban ser reportados.

Para concluir, y en consideración de la entrada en vigencia de la Ley Marco de Ciberseguridad, el llamado es a prepararse por parte de las organizaciones, especialmente aquellas que prestan servicios esenciales como posibles instituciones que puedan ser operadores de importancia vital, pero no limitándose a estos, sino también aquellos proveedores que se relacionan con estas organizaciones y por ende, que se encuentran dentro de la cadena de suministro que pudiesen verse afectados ante a un ciberataque o incidente de ciberseguridad..

---

Para más información, contactar a:

**Juan Pablo González**
Director
Protección de Datos Personales, Ciberseguridad y Nuevas Tecnologías
jpgonzalez@hdgroup.cl

---