alerta legal

Nuevas Regulaciones en la Ley Marco sobre Ciberseguridad

El 13 de marzo de 2025 se publicó en el Diario Oficial el Decreto Supremo N°285 que aprueba el "Reglamento del Procedimiento de Calificación de los Operadores de Importancia Vital de la Ley N°21.663" (el Reglamento). Este Reglamento complementa la Ley Marco sobre Ciberseguridad e Infraestructura Crítica ("LMC"), promulgada el 26 de marzo de 2024, la cual establece la institucionalidad, principios y requisitos mínimos necesarios para coordinar las acciones de ciberseguridad en el país. La LMC regula tanto a los organismos del Estado como a los particulares, definiendo las obligaciones de las instituciones que prestan servicios esenciales y consolidándose como un marco integral para enfrentar los desafíos de ciberseguridad en Chile.

I. Sobre los Operadores de Importancia Vital (OIV)

El Reglamento regula el procedimiento de calificación de los "Operadores de Importancia Vital" (OIV), según lo dispuesto en los artículos 5° y 6° de la LMC. Esta calificación será realizada por la Agencia Nacional de Ciberseguridad (ANCI) y aplica a instituciones que presten servicios calificados como "esenciales" conforme al artículo 4° de la ley.

El reglamento establece los siguientes requisitos para ser considerado OIV:

- Que la provisión del servicio dependa de redes y sistemas informáticos.
- Que su afectación, interceptación, interrupción o destrucción 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.

Además, detalla los criterios que la ANCI deberá considerar para determinar el impacto, y que son (1) número de potenciales afectados, (2) la monoprovisión[1], (3) la redundancia del servicio[2], (4) la dependencia de los servicios proveídos entre sí o con otros servicios esenciales[3] Y, (5) la relevancia de la institución que pudiera verse afectada.

Se permite también que la ANCI designe como OIV a empresas privadas que no sean servicios esenciales en las condiciones que establece el Reglamento, según lo permite el artículo 5°, inciso segundo de la LMC.

El proceso de calificación se iniciará el 30 de mayo de 2025, cuando la ANCI solicite informes técnicos a organismos reguladores sectoriales sobre las instituciones públicas y privadas que puedan ser calificadas como OIV en sus respectivos ámbitos de competencia. Estos organismos tendrán un plazo de 30 días corridos para entregar los informes. Posteriormente, la ANCI contará con otros 30 días para elaborar una nómina preliminar de OIV, la que será sometida a consulta pública por un periodo adicional de 30 días, a través de una plataforma electrónica.

Es relevante recalcar que en contra de la Resolución de la ANCI que determine la calificación final de los OIV, podrán deducirse los recursos establecidos en la Ley 19.880 (sobre bases del procedimiento administrativo), además de la reclamación judicial prescrita en el artículo 46 de la LMC, en contra de resoluciones finales o de término de la ANCI que sean ilegales y cause perjuicio al interesado, acción que se debe ejercer ante la Corte de Apelaciones competente.

II. Reporte de Incidentes de Ciberseguridad

Por otro lado, el pasado 1 de marzo se publicó en el Diario Oficial el Decreto Supremo N°295 que "Aprueba Reglamento de Reporte de Incidentes de Ciberseguridad de la Ley N°21.663". **Desde ese momento es obligatorio para las instituciones que presenten servicios esenciales (según el art. 4 de la Ley) reportar a la ANCI los ciberataques o incidentes de impacto significativo.** Este reglamento obliga a estas instituciones a reportar dentro del plazo máximo de 3 horas desde el conocimiento de la vulneración.

1 Característica de un servicio esencial en la que existe un único proveedor.
2 Condición en la que una persona natural o jurídica puede reemplazar de manera inmediata la provisión de un servicio esencial por algún proveedor alternativo, en caso de que este sea afectado o interrumpido.
3 Según el artículo 2°, letra b) del Reglamento, Dependencia es: "Relación entre dos operadores en la que uno de ellos no puede proveer su servicio si no recibe un bien o servicio de otro".

Asimismo, se encarga de establecer el procedimiento específico para notificar el incidente, forma, condiciones de anonimato, taxonomía del informe, información mínima y la periodicidad de los reportes.

Este reglamento desarrolla el mandato del artículo 9° de la Ley, que impone a estas instituciones, ya sean públicas o privadas, el deber de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos del artículo 27°, es decir, aquellos incidentes capaces de 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.

A su vez, se publicó Resolución Exenta N°7 de 2025 que "Aprueba Taxonomía de Incidentes de Ciberseguridad", cumpliendo con el mandato del artículo 5° letra f) del Decreto Supremo N°295, el cual exige incluir en los informes una descripción del incidente, si este puede ser identificado.

La resolución establece lineamientos técnicos que clasifican los incidentes según cuatro áreas de impacto: afectación al uso legítimo de recursos, confidencialidad de la información, disponibilidad de servicios esenciales e integridad de la información.

Adicionalmente, se definen once efectos observables para categorizar los incidentes[1], algunos de ellos son el uso no autorizado de redes y sistemas informáticos, actividades de phishing o fraude, ejecución no autorizada de código, exposición de datos, indisponibilidad de servicio, modificación no autorizada de datos.

De este modo, la resolución exenta categoriza los potenciales incidentes, permitiendo que las instituciones puedan identificar y reportar de qué se tratan de manera más sencilla y expedita.

Las nuevas normativas publicadas en el marco de la LMC refuerzan el ecosistema regulatorio para garantizar una gestión efectiva de la ciberseguridad en Chile. Es crucial que las instituciones sujetas a esta legislación revisen su cumplimiento.

Revisa otras alertas legales preparadas por Guerrero Olivos sobre la Ley Marco de Ciberseguridad:

- Nueva Ley Marco de Ciberseguridad en Chile: Entrada en Vigencia y Creación de la Agencia Nacional de Ciberseguridad
- Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información

4 Todo contexto, escenario o circunstancia que pueda ser observada directamente, independiente de su causa u origen.

contacto

Diego Morandé
dmorande@guerrero.cl

Alejandra Leiton
aleiton@guerrero.cl

Valentina Mora
vmora@guerrero.cl

Antonia Paredes
aparedes@guerrero.cl

Hannelore Rennke
hrennke@guerrero.cl

Leonardo Tore
ltore@guerrero.cl

Joaquín Valenzuela
jvalenzuelac@guerrero.cl