



JAIME HIRSCHBERG



JORGE ARANCIBIA

Entra en vigencia la Ley N° 21.663, “Ley Marco de Ciberseguridad”, la cual establece los nuevos principios, institucionalidad y normativa general en materia de ciberseguridad, tanto para organismos del Estado como para entidades privadas.

El día 1 de enero de 2025, entró en vigencia la Ley N° 21.663, Ley Marco de Ciberseguridad. Esto ocurre aproximadamente una semana después de la publicación, en el Diario Oficial del 24 de diciembre de 2024, del primer reglamento de la Ley, que fijó la fecha para el inicio de actividades de la Agencia Nacional de Ciberseguridad (en adelante, la “Agencia”), entidad creada por la misma Ley.

La Ley tiene como objetivo principal establecer la institucionalidad, los principios y la normativa general que permitirán estructurar, regular y coordinar las acciones de ciberseguridad tanto en los organismos del Estado como entre estos y las entidades privadas. Abarca, además, la definición de los requisitos mínimos que deben cumplir las instituciones para la prevención, contención, resolución y respuesta ante incidentes de ciberseguridad.

En particular, la Ley se aplicará a las instituciones que presten servicios calificados como esenciales según lo establecido en los incisos segundo y tercero de su artículo 4° y a aquellas que sean calificadas como operadores de importancia vital, de conformidad con lo dispuesto en los artículos 5° y 6°.

Son servicios esenciales, y por lo tanto, deben observar los deberes establecidos en la Ley, aquellos servicios provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional; los prestados bajo concesión de servicio público, y los proveídos por instituciones privadas que realicen las siguientes actividades: generación, transmisión o distribución eléctrica; 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 infraestructura respectiva; banca, servicios financieros y medios de pago; administración de prestaciones de seguridad social; servicios

postales y de mensajería; prestación institucional de salud por entidades tales como hospitales, clínicas, consultorios y centros médicos, y la producción y/o investigación de productos farmacéuticos.

Por otro lado, la Agencia podrá calificar como operadores de importancia vital a quienes reúnan los siguientes requisitos: (i) Que la provisión de dicho servicio dependa de las redes y sistemas informáticos; y (ii) Que 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.

Las instituciones obligadas por la Ley deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso. Para el caso de los operadores de importancia vital, estos deberán observar los deberes particulares que establece la Ley para estos.

Como se mencionó anteriormente, la Ley también creó la Agencia Nacional de Ciberseguridad, entidad encargada de fiscalizar el cumplimiento de esta.

Por último, recordar que esta Ley establece un régimen nuevo de infracciones y sanciones, con multas de hasta 20.000 unidades tributarias mensuales para los servicios calificados como esenciales y de hasta 40.000 unidades tributarias mensuales para los operadores de importancia vital.

Dudas sobre este tema contacta a:
Jaime Hirschberg / jhirschberg@riedfabres.cl
Jorge Arancibia / jarancibia@riedfabres.cl