Alerta Legal: Cinco claves para entender la futura Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información

13 de diciembre de 2023 | *Por* Jorge Timmermann *y* Carla Illanes.

El 12 de diciembre de 2023, el Senado aprobó y despachó el proyecto de ley sobre Ciberseguridad e Infraestructura Crítica de la Información, el cual deberá ir al Tribunal Constitucional para posteriormente convertirse en ley.

Dicha normativa se aplicará a aquellas instituciones que presten servicios calificados por la nueva Agencia Nacional de Ciberseguridad (ANCI), como Servicios Esenciales (SE) o como Operadores de Importancia Vital (OIV). Todos los obligados deberán reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos tan pronto les sea posible y conforme los plazos que ahí se establecen.

I. Servicios Esenciales (SE)

a. Servicios suministrados por organismos de la **Administración del Estado** y el **Coordinador Eléctrico Nacional**.

b. Servicios ofrecidos mediante **concesión de servicio público.**

c. Servicios proporcionados por **entidades privadas** involucradas en actividades como generación, transmisión o distribución eléctrica, transporte y almacenamiento de combustibles, suministro de agua potable o saneamiento,

telecomunicaciones, infraestructura digital, servicios digitales, servicios de tecnología de la información gestionados por terceros, transporte terrestre, aéreo, ferroviario o marítimo, operación de su infraestructura, banca, servicios financieros, medios de pago, administración de prestaciones de seguridad social, servicios postales y de mensajería, prestación institucional de salud y producción o investigación de productos farmacéuticos.

La ANCI podrá designar **otros servicios, infraestructuras, procesos o funciones** como servicios esenciales cuando su impacto pueda ocasionar daños graves a: la vida o integridad física de la población, el abastecimiento, los sectores clave de la actividad económica, el medioambiente, el funcionamiento normal de la sociedad, la Administración del Estado, la defensa nacional o la seguridad y el orden público. Esta designación estará sujeta a consulta pública.

II. Operadores de Importancia Vital (OIV)

Se consideran OIV aquellos SE que cumplen con los siguientes requisitos:

a. Que su provisión dependa de **redes y sistemas informáticos**.

b. Que la afectación, interceptación, interrupción o destrucción de sus servicios tengan un **impacto significativo** en: la seguridad y el orden público, la provisión continua y regular de servicios esenciales, el cumplimiento efectivo de las funciones del Estado general, los servicios que este debe proveer o garantizar.

Adicionalmente, la ANCI podrá calificar como OIV a aquellos entes privados que cumplan con los requisitos descritos y que hayanadquirido un rol esencial en el abastecimiento de la población, la distribución de bienes o la producción de aquellos indispensables o estratégicos para el país. .

Entre otras obligaciones, los OIV deberán implementar un sistema de gestión de seguridad de la información continuo; elaborar, implementar y certificar planes de continuidad operacional y ciberseguridad y designar un delegado de ciberseguridad.

III. Creación de la ANCI

Se establecerá un servicio público descentralizado para garantizar la coherencia normativa en materia de ciberseguridad, la ANCI.

Su función principal será asesorar al presidente de la República en la formulación y aprobación de la Política Nacional de Ciberseguridad, supervisando planes y emitiendo protocolos obligatorios para instituciones públicas y privadas. Entre sus atribuciones, estarán: calificar los SE y OIV, iniciar procedimientos sancionatorios y aplicar sanciones por incumplimientos de los sujetos obligados.

IV. Nuevo régimen de infracciones y multas

Las infracciones a las obligaciones establecidas por la ley para los sujetos obligados serán clasificadas en tres categorías: **leves, graves y gravísimas**. Esta clasificación abarcará desde casos leves, como la entrega tardía de información que no sea necesaria para la gestión de un incidente de ciberseguridad; hasta situaciones graves, como el incumplimiento de la obligación de reportar. Asimismo, se considerará gravísima la acción de proporcionar a la Agencia información evidentemente falsa o errónea, especialmente cuando dicha información sea necesaria para la gestión de un incidente de ciberseguridad.

La infracción a los preceptos de la ley conllevará la imposición de una multa a beneficio fiscal que irá entre las **5.000 y 40.000 UTM**, dependiendo de la entidad de la infracción y del sujeto obligado (las multas serán más significativas en el caso de OIV).

V. Entrada en vigencia

Según lo dispuesto en el artículo primero transitorio, se otorga al presidente de la República la facultad de emitir, dentro del plazo de un año, uno o más decretos con fuerza de ley. Estos decretos tendrán como objetivo fijar la fecha de inicio de actividades de la ANCI y establecer un periodo de vigencia para las normas contempladas por la ley, el cual no podrá ser menor a seis meses a partir de su publicación.

	Contacto: Para más información, por favor contactar a: Carla illanes Counsel carla.illanes@dlapiper.cl

**Este reporte provee de información general sobre ciertas cuestiones de carácter legal o comercial en Chile y no tiene por fin analizar en detalle las materias contenidas en este, ni tampoco está destinado a proporcionar una asesoría legal particular sobre las mismas. Se sugiere al lector buscar asistencia legal antes de tomar una decisión relativa a las materias contenidas en el presente informe. Este informe no puede ser reproducido por cualquier medio o en parte alguna sin el consentimiento previo de DLA Piper Chile 2023.*