Cariola Díez
Pérez-Cotapos

ALERTA LEGAL

PROYECTO DE LEY MARCO DE CIBERSEGURIDAD

1) Proyecto de Ley Marco de Ciberseguridad

El proyecto de ley sobre Ciberseguridad e Infraestructura Crítica de la Información, aprobado por el Senado el 12 de diciembre de 2023 y que únicamente tiene pendiente su revisión por el Tribunal Constitucional para ser promulgado y publicado en el diario oficial como ley, **establece una nueva institucionalidad para fortalecer la seguridad digital y enfrentar contingencias en el ciberespacio.** El proyecto, inspirado en la Directiva NIS2 de la Unión Europea, crea un **modelo de gobernanza basado en colaboración público-privada,** incluye una **Agencia Nacional de Ciberseguridad** (ANCI o Agencia), un **Consejo Multisectorialsobre Ciberseguridad**, un **Comité Interministerial sobreCiberseguridad** y **equipos de respuesta a incidentesde seguridad informática** (**CSIRTs**, tanto uno Nacional al interior de la ANCI como uno de Defensa Nacional, así como CSIRTs que pudieran pertenecer a organismos de la Administración del Estado), siguiendo estándares internacionales.

La novedad más significativa es el **rol preponderante que se entrega a los privados en la infraestructura de ciberseguridad del país**. Esto se manifiesta principalmente en las obligaciones que se imponen a los operadores de importancia vital que prestan servicios esenciales.

2) Ámbito de Aplicación

El proyecto establece su aplicación a instituciones públicas y privadas que proveen **servicios esenciales y a operadores de importancia vital**, estando sujetos los primeros a deberes generales, y los segundos a dichas deberes generales y, además, a otros especiales.

A) ¿Qué es un prestador de servicio esencial?

El proyecto busca proteger mediante un marco general los denominados **prestadores de servicios esenciales**. Los servicios esenciales son:

1) Los ofrecidos 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, 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**.

2) Los proporcionados por **los Organismos de la Administración del Estado y el Coordinador Eléctrico Nacional**; y

3) Los prestados bajo **concesión de servicio público**.

La Agencia puede designar adicionalmente otros servicios como esenciales si su afectación puede causar un grave daño (i) a la vida o a la integridad física de la población o a su abastecimiento, (ii) a sectores relevantes de las actividades económicas, (iii) al medioambiente, (iv) al normal funcionamiento de la sociedad y/o de la Administración del Estado, (v) a la defensa nacional, o (vi) a la seguridad y el orden público. Esta designación se realizará luego de un proceso de consulta pública.

Estos deberán dar cumplimiento a los **deberes generales** de ciberseguridad que establece el proyecto:

1) Estarán obligadas a **implementar medidas continuas de prevención, reporte y resolución de incidentes de ciberseguridad**, que pueden ser tecnológicas, organizacionales, físicas o informativas.

2) Deberán cumplir con los **protocolos y estándares de ciberseguridad establecidos por la Agencia y la normativa sectorial específica**, enfocados en la prevención y gestión de riesgos, y en la contención y mitigación del impacto de los incidentes en la operatividad y seguridad de la información.

Para dictar los protocolos y estándares la Agencia deberá mantener **coordinación con autoridades sectoriales**, someter los instrumentos a consulta pública y, además, establecer medidas **diferenciadas según el tipo de organización de que se trate, por ejemplo, de acuerdo al tamaño del prestador de servicios.**

B) ¿Qué es un operador de importancia vital?

Estas son instituciones que, mediante resolución fundada, sean designadas por el Director de la Agencia, **cumpliendo con dos requisitos**:

1) **Dependencia de la provisión de sus servicios en redes y sistemas informáticos**; y
2) **Impacto significativo** en la seguridad; el orden público; la continuidad y regularidad de servicios esenciales; o en las funciones del Estado (o en los servicios que debe proveer o garantizar) derivado de afectaciones a sus servicios.

Además, la Agencia puede designar a instituciones privadas que no sean prestadoras de servicios esenciales, pero que cumplan con los dos requisitos ya indicados y cuya calificación como operador de importancia vital sea indispensable por su rol crítico en el abastecimiento de la población, la distribución de bienes o la producción de aquellos indispensables o estratégicos para el país, o por el grado de exposición a riesgos de ciberseguridad.

El proceso de calificación de operadores de importancia vital será revisado y actualizado cada 3 años por la ANCI.

Además de estar sujetos a los **deberes generales** antes indicados, los operadores de importancia vital estarán obligados a los siguientes **deberes especiales** de ciberseguridad:

1) Implementación de un **sistema de gestión de seguridad** de la información para evaluar riesgos en redes y sistemas informáticos.

2) Mantenimiento de un **registro de acciones** del sistema de gestión, elaboración y certificación de **planes de continuidad operacional y ciberseguridad**, y realización de **revisiones y simulacros periódicos**.

3) Adopción de **medidas para reducir el impacto de incidentes** de ciberseguridad, **notificación de incidentes a afectados**, programas de **capacitación** en ciberseguridad, y designación de un **delegado** de ciberseguridad.

3) Reporte de Ciberataques y de Incidentes de Ciberseguridad de Instituciones Públicas y Privadas

Las instituciones públicas y privadas obligadas -es decir, incluyendo tanto a los prestadores de servicios esenciales como a los operadores de importancia vital- tendrán la **obligación de reportar al CSIRT Nacional**:

1) Los **ciberataques**, que son definidos como "*intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático*".

2) Los **incidentes de ciberseguridad que puedan tener efectos significativos**. Los incidentes de ciberseguridad son definidos de manera amplia como "*todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes o sistemas informáticos, o la autenticación o no-repudio de los procesos ejecutados o implementados en las redes o sistemas informáticos*". El proyecto considera que existe este efecto significativo si el incidente "*es capaz 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, para determinar la importancia de los efectos de un incidente el proyecto establece como criterios: (i) el número de personas afectadas, (ii) la duración del incidente y (iii) la extensión geográfica con respecto a la zona afectada por el incidente.

El **reporte deberá ser enviado al CSIRT tan pronto sea posible y conforme al esquema sintetizado en el siguiente cuadro**, cuyos plazos se cuentan desde que se tiene conocimiento del incidente o ciberataque:

Situación / Tipo de Reporte	Alerta Temprana	Actualización y evaluación inicial del incidente, gravedad e impacto	Informe final (o informe de situación si incidente sigue en curso)
Instituciones públicas y privadas	Máximo **3** horas	Máximo **72** horas	Máximo **15** días
Operador de Importancia vital que vea afectada prestación de servicios esenciales	Máximo **3** horas	Máximo **24** horas	Máximo **15** días

Los operadores de importancia vital deberán, además, **informar al CSIRT Nacional su plan de acción** tan pronto lo hubieran adoptado, el cual **no podrá ser adoptado en un plazo superior a 7 días** corridos desde que se tuvo conocimiento del incidente.

4) Sanciones y Procedimiento Sancionatorio

La ley establece **infracciones leves, graves y gravísimas**, las que prescriben en 3 años. Las **multas llegan hasta las 40.000 UTM**. Para fijar la multa se considerará:

1) El **grado en que el infractor adoptó las medidas** necesarias para resguardar la seguridad informática.
2) La **probabilidad** de ocurrencia del incidente.
3) El **grado de exposición** a los riesgos.
4) La **gravedad de los efectos** de los ataques (incluyendo repercusiones sociales o económicas).
5) La **reiteración** en la infracción en los últimos 3 años.
6) El **tamaño y capacidad económica** del infractor.

Cuando una infracción también pueda ser sancionada conforme a otra ley, **se impondrá la sanción de mayor gravedad**. En ningún caso se impondrán dos o más sanciones administrativas por los mismos hechos y fundamentos jurídicos.

El proyecto contempla un **procedimiento sancionatorio a cargo del subdirector de la Agencia** y que se rige por la Ley N° 19.980 de Bases de los Procedimientos Administrativos y por ciertas reglas específicas establecidas en el mismo. **Corresponderá al subdirector decidir el procedimiento, emitiendo una resolución que incluya el mismo contenido del informe del instructor del procedimiento.** La resolución de término será recurrible administrativa y judicialmente. Para el último propósito, las personas que estimen que la resolución es ilegal y que les causa perjuicio podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante. Contra la decisión de la Corte de Apelaciones se podrá apelar ante la Corte Suprema.

5) Entrada en Vigencia e Implementación

El proyecto autoriza al Presidente de la República a establecer mediante uno o más decretos dictados en el plazo de un año desde la publicación de la ley:

1) **La fecha para la iniciación de actividades de la Agencia**, pudiendo contemplar un período para su implementación y uno a contar del cual entrará en operaciones.

2) **Un período para la vigencia de la ley**, el cual **no podrá ser inferior a seis meses** desde su publicación.

De manera excepcional, el **Presidente de la República podrá nombrar al primer Director de la Agencia**, quien asumirá de inmediato, durará como máximo un año en el cargo y no podrá participar en el proceso de selección por Alta Dirección Pública de su sucesor.

Finalmente, dentro del plazo de **180 días posteriores a la publicación de la ley, el Ministerio del Interior y Seguridad Pública dictará los reglamentos señalados en la misma**.

Cariola Díez
Pérez-Cotapos

CONTACTO

Rodrigo Lavados

Socio

Gabriel Pensa

Asociado Senior

Eduardo Vilches

Asociado Senior