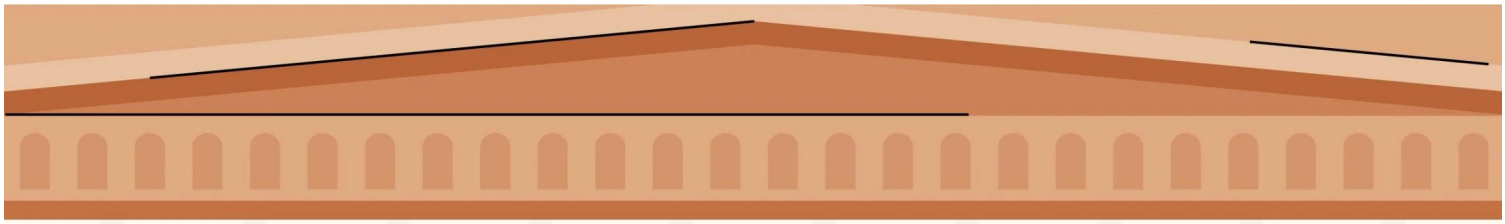

CHILE
Ley Marco de Ciberseguridad y Agencia Nacional: pilares de la nueva institucionalidad
2024



A pocos meses de que comience a regir la Ley 21.663 que establece el nuevo marco regulatorio en Chile, el Coordinador Nacional de Ciberseguridad, Daniel Álvarez Valenzuela, releva los avances alcanzados e invita a los actores, tanto públicos, como privados, a prepararse para la inminente puesta en marcha de la ley.

Este 2025 comenzará a regir la Ley Marco de Ciberseguridad, hecho histórico que posiciona a nuestro país como líder en regulación en esta materia en América Latina y El Caribe. Sin embargo, también implica una serie de desafíos para el ecosistema nacional, que deben asumirse desde ya, como parte de la preparación para su puesta en marcha.

El Coordinador Nacional de Ciberseguridad, Daniel Álvarez Valenzuela, explica que el nuevo cuerpo legal permitirá que Chile se convierta en el primer país de esta parte del planeta en contar con una autoridad nacional de ciberseguridad, que tendrá facultades regulatorias, fiscalizadoras y sancionatorias, tanto respecto de los organismos públicos, como privados.

El proceso de implementación resulta de gran relevancia para Álvarez, pues implicará una preparación del ecosistema en general, con el fin de que la llegada de la nueva institucionalidad "genere un círculo virtuoso del que todos podamos aportarnos y beneficiarnos".

La Ley Marco de Ciberseguridad, explica el Coordinador Nacional, tiene entre sus principales reglas crear el sistema de gobernanza pública en esta materia, creado la Agencia Nacional de Ciberseguridad (ANCI); los CSIRT Nacional y de Defensa; la Red de Conectividad Segura del Estado; el Consejo Multisectorial y el Comité Interministerial. Además, fija principios y normas generales para estructurar, regular y coordinar las acciones de ciberseguridad.

Álvarez precisa que uno de los objetivos de la Ley 21.663 es la creación de esta institucionalidad en ciberseguridad, lo que ha resultado fundamental en la experiencia de los países líderes en la materia, debido a que permite contar con "un agente público a cargo de proveer, no solo la respuesta a incidentes, uno de los objetivos principales, sino también de promover la concientización, la educación y las políticas, pues debemos entender que la ciberseguridad no solo es un asunto técnico, sino que también una materia de políticas públicas", expresa.

"un agente público a cargo de proveer, no solo la respuesta a incidentes, uno de los objetivos principales, sino también de promover la concientización, la educación y las políticas, pues debemos entender que la ciberseguridad no solo es un asunto técnico, sino que también una materia de políticas públicas"

El desarrollo del correspondiente marco regulatorio para la puesta en marcha de esta institucionalidad es otro gran objetivo de este cuerpo legal, ya que con él será posible contar con estándares de ciberseguridad aplicables a todos los actores del país, gracias a la facultad normativa de la nueva Agencia.

El Coordinador Nacional de Ciberseguridad afirma que otro objetivo de la Ley Marco es la respuesta a incidentes. "La obligación de los servicios esenciales de notificar los incidentes de impacto significativo permitirá contar con una visión holística y actualizada de la situación de seguridad digital del país, facilitando la respuesta y mitigación de los ciberataques", afirma, enfatizando que "notificar incidentes nos pone en una mejor situación de ciberseguridad, porque la seguridad es colectiva, no individual".

Cabe señalar que el Equipo Nacional de Respuesta ante Incidentes de Seguridad Informática (CSIRT) Nacional, que dependerá de la ANCI, tendrá entre sus funciones específicas: responder ante ciberataques o incidentes de ciberseguridad relevantes; coordinar a los nuevos CSIRT que se crearán para las distintas ramas del Estado, incluyendo el CSIRT de la Defensa Nacional; colaborar con entidades extranjeras en el intercambio de información; entregar asesoría técnica para la implementación y realización de acciones que permitan una mayor ciberseguridad en las instituciones del Estado, entre otras.

Algunos detalles de la nueva institucionalidad

Entre los puntos más relevantes de la nueva institucionalidad en ciberseguridad se encuentra la identificación de quiénes son los Servicios esenciales y Operadores de Importancia Vital (OIV) en el país.

Álvarez explica que "la ley define 13 servicios esenciales: gobierno, sector eléctrico, sanitario, combustibles, transporte, telecomunicaciones, infraestructura digital, servicios digitales y servicios TI, bancarios y financieros, seguridad

social, correos, servicios institucionales de salud, producción o investigación farmacéutica", lo que tendrán dos deberes fundamentales: adoptar medidas para prevenir, resolver y reportar incidentes de ciberseguridad y notificar al CSIRT Nacional aquellos incidentes con efectos significativos.

Por otro lado, los Operadores de Importancia Vital (OIV) serán aquellos prestadores de servicios esenciales cuya operación dependa de las redes y sistemas informáticos y que por su afectación o interrupción tengan un impacto significativo en la seguridad y orden público, en la provisión continua y regular de servicios esenciales y en el efectivo cumplimiento de las funciones del Estado.

La ANCI además podrá clasificar como OIV a instituciones privadas que, aunque no estén directamente vinculadas a la prestación de servicios esenciales, hayan adquirido un rol crítico en el abastecimiento de la población, la distribución de bienes o la producción de insumos estratégicos para el país.

La Ley Marco impone a las instituciones que presten servicios esenciales y a los OIV una serie de obligaciones clave para asegurar la protección de sus sistemas y redes ante potenciales ciberataques. Estas medidas deberán aplicarse de manera continua y son de carácter preventivo, correctivo y organizacional.

Adicionalmente, las OIV también tendrán los siguientes deberes específicos:

- Implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar riesgos
- Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de seguridad de la información.
- Elaborar e implementar planes de continuidad operacional y ciberseguridad.
- Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y sistemas.
- Adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad.
- Contar con certificaciones.
- Informar a los potenciales afectados.
- Contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene.
- Designar un delegado de ciberseguridad.

Con la implementación de la Ley Marco de Ciberseguridad, Chile se posiciona a la vanguardia de la regulación en esta materia en Latinoamérica y El Caribe, estableciendo un marco normativo robusto que busca proteger a las personas, fundamentalmente, y a las instituciones frente a las amenazas cibernéticas. Este cuerpo legal no solo fortalece la resiliencia del país frente a ataques digitales, sino que también fomenta una cultura de la ciberseguridad, contribuyendo al desarrollo de una sociedad más segura y preparada en el ámbito digital.