# Protección de datos y ciberseguridad

El Congreso chileno aprobó, tras 7 años de tramitación, el proyecto de la ley de Protección de Datos Personales que sigue los estándares establecidos en el Reglamento General de Protección de Datos de la Unión Europea y crea la Agencia de Protección de Datos con el objetivo de fiscalizar su cumplimiento y aplicar sanciones. Esta Ley, cuyo texto definitivo está pendiente de publicación, permitirá a Chile ser declarado por la Comisión Europea como país con un nivel adecuado de protección de datos personales, lo que facilitará la transferencia internacional de datos entre Chile y la Unión Europea. La nueva ley entrará en vigor 24 meses después de su publicación para adaptarse al nuevo régimen.

En la Unión Europea, por su parte, se publicó el Reglamento en el que se detallan los casos en que un incidente se considera significativo y que obliga a las entidades a notificar dichos incidentes. Destacar, entre otros, (i) que el incidente haya causado o pueda causar a la entidad pertinente pérdidas financieras directas superiores a 500.000 EUR o al 5% de su volumen de negocios total anual en el ejercicio financiero anterior, (ii) que un servicio de computación en nube esté totalmente indisponible durante más de treinta minutos, (iii) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con la prestación de un servicio de computación en nube se vean comprometidas como consecuencia de una acción presuntamente malintencionada.

# Actualización de las medidas europeas sobre ciberseguridad

El 27 de junio entró en vigor el Reglamento de la Unión Europea del Parlamento Europeo relativo a la Agencia de la Unión Europea para la Ciberseguridad y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación.

La norma, que deroga el anterior Reglamento sobre la Ciberseguridad del 2013, tiene como aspiración alcanzar un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión Europea.

A continuación destacamos los dos bloques fundamentales del documento:

## Agencia Europea para la Ciberseguridad

En primer lugar, el Reglamento establece los objetivos y aspectos organizativos de la nueva Agencia Europea para la Ciberseguridad (ENISA), y le asigna las siguientes tareas:

Contribuir a la elaboración y ejecución de la política y del derecho de la Unión en el ámbito de la ciberseguridad
Asistir a los Estados en la creación de capacidades de ciberseguridad
Apoyar la cooperación entre los países miembros, las instituciones, órganos y organismos de la Unión y entre las partes interesadas
Promover el desarrollo y la aplicación de la política de la UE en materia de certificación de la ciberseguridad de productos, servicios y procesos TIC
Analizar las tecnologías emergentes y preparar evaluaciones sobre los efectos esperados, de tipo social, jurídico, económico y reglamentario, de las innovaciones tecnológicas
Sensibilizar al público sobre los riesgos relacionados con la ciberseguridad y facilitar orientaciones sobre buenas prácticas
Asesorar a las instituciones, órganos y organismos de la Unión y a los Estados miembros sobre las necesidades y prioridades de la investigación en el ámbito de la ciberseguridad y las tecnologías de la información, y a utilizar eficazmente las tecnologías de prevención del riesgo
Promover la cooperación internacional en relación con los problemas que se refieren a la ciberseguridad

## Certificación de la ciberseguridad

Por otra parte, aborda la definición de un marco para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de las tecnologías de la información y la comunicación (TIC) y de crear un mercado único digital para estos productos, servicios y procesos.

Este marco define un mecanismo destinado a instaurar esquemas europeos de certificación de la ciberseguridad y a confirmar que los productos, servicios y procesos de TIC que hayan sido evaluados con arreglo a dichos esquemas, cumplen los requisitos de seguridad especificados. De esta manera se trata de proteger la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen.

La Comisión Europea publicará un programa de trabajo evolutivo para los esquemas europeos de

certificación que definirá las prioridades estratégicas para los futuros esquemas e incluirá una lista de productos, servicios y procesos de TIC, o de categorías de los mismos, que pudieran beneficiarse de su inclusión en el ámbito de aplicación de un esquema europeo de certificación de la ciberseguridad.