A la vanguardia en materia de ciberseguridad

Nueva Ley Marco de Ciberseguridad en Chile

Todo lo que debes saber

Agosto 2024

Índice

01. ¿Qué implica la nueva Ley Marco de Ciberseguridad de Chile?

El Senado de Chile aprobó y publicó la nueva Ley Marco sobre Ciberseguridad el pasado 8 de abril de 2024, como parte de su agenda de seguridad pública. Esta legislación tiene como objetivo establecer una nueva institucionalidad para fortalecer la ciberseguridad en el país y promover una cultura pública de seguridad en el ciberespacio.
A continuación, te explicamos las implicaciones de esta nueva Ley Marco de Ciberseguridad y cómo puedes preparar a tu empresa para cumplir con sus requisitos

La Ley Marco de Ciberseguridad, publicada en el Diario Oficial de Chile, establece una normativa general que regula cómo las instituciones públicas y privadas deben enfrentar los desafíos de ciberseguridad. Su finalidad es **mejorar la prevención y resolución de delitos informáticos e incidentes de ciberseguridad.**
Con esta legislación, Chile se posiciona como uno de los primeros países de Latinoamérica en desarrollar un proyecto de ley de esta magnitud en el ámbito de la ciberseguridad.
Uno de los aspectos centrales de la ley es la obligación de **notificar incidentes de ciberseguridad a nuevas instituciones creadas específicamente** para este propósito.
A continuación, presentamos un resumen de sus implicaciones más destacadas:

Nueva institucionalidad

La nueva ley aborda la necesidad de crear instituciones que garanticen su correcta aplicación y regulación. Entre estas instituciones destacan:

Agencia Nacional de Ciberseguridad (ANCI):	Esta entidad técnica se dedica a proteger los intereses chilenos en el ciberespacio y cuenta con facultades reguladoras, sancionadoras y fiscalizadoras.
Consejo Multisectorial sobre Ciberseguridad:	Su función es asesorar a la ANCI mediante el análisis periódico de la situación de ciberseguridad y la formulación de medidas para su mejora.
Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional):	Definidos como centros multidisciplinarios, su responsabilidad es prevenir, identificar y responder a ciberataques de manera rápida y efectiva, mitigando sus efectos. Las instituciones sujetas a la ley deberán notificar al CSIRT cualquier evento que comprometa la seguridad de infraestructura crítica y datos personales.
CSIRT de la Defensa Nacional	Este organismo se encarga de proteger los sistemas informáticos de los servicios de defensa de la nación, como las Fuerzas Armadas, y colaborar con el CSIRT Nacional en caso de ataques cibernéticos que afecten la seguridad pública nacional.
Red de Conectividad Segura del Estado:	Diseñada para proporcionar una conexión segura a Internet y entre dispositivos de los organismos de la Administración del Estado, su correcto funcionamiento será supervisado por la ANCI.

Además, la ley implica la modificación de otros cuerpos legales existentes para mantener la coherencia y evitar vacíos legales.

Obligaciones y derechos

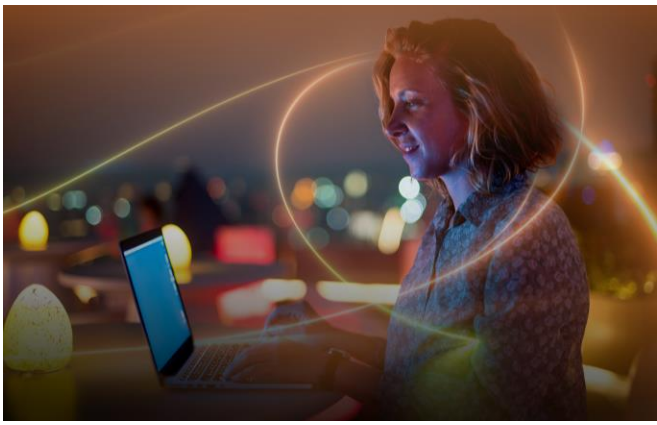
La nueva ley establece que las entidades sujetas a ella deben desarrollar y aplicar protocolos para prevenir, reportar y resolver incidentes de ciberseguridad. Estas obligaciones incluyen:

- **Implementar un sistema de gestión de seguridad de la información (SGSI) continuo,** capaz de evaluar la probabilidad y el impacto de incidentes de ciberseguridad.
- **Mantener un registro detallado de** las acciones realizadas dentro del SGSI.
- **Crear y actualizar planes de continuidad operacional,** al menos cada dos años.
- **Informar a los potenciales afectados** sobre ciberataques que puedan comprometer su acceso a redes y sistemas informáticos, así como aquellos que involucren sus datos personales.
- **Realizar revisiones continuas,** incluyendo pruebas de penetración (pentesting), para la detección temprana de posibles vulnerabilidades.
- **Tomar medidas oportunas** para reducir el impacto y la propagación de incidentes de ciberseguridad.
- **Obtener certificaciones** nacionales e internacionales en ciberseguridad.
- **Designar un delegado de ciberseguridad,** ya sea interno o subcontratado, responsable de informar a la autoridad competente sobre incidentes de ciberseguridad.

Además, todas las instituciones públicas y privadas cubiertas por esta ley deben reportar al Equipo Nacional de Respuesta los ciberataques e incidentes de ciberseguridad que puedan tener un impacto significativo en el funcionamiento del país y sus instituciones.

Sanciones

La ley también define varios tipos de infracciones y las consecuencias por incumplir las obligaciones establecidas. Esto incluye multas que oscilan entre 5.000 y 40.000 unidades tributarias mensuales (UTM), dependiendo de la gravedad de la infracción cometida.



02. Objetivos Política Nacional de Ciberseguridad

En la era digital, la ciberseguridad es esencial para proteger a los ciudadanos y las infraestructuras críticas. Chile ha definido una estrategia que incluye la creación de una infraestructura resiliente, la promoción de los derechos de las personas en Internet, el desarrollo de una cultura de ciberseguridad, la coordinación nacional e internacional, y el fomento de la industria y la investigación en ciberseguridad. Esta visión integral busca asegurar un entorno digital seguro y próspero para todos.

01.
Infraestructura resiliente

El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad y de desastres socioambientales, bajo una perspectiva de gestión de riesgos.

02.
Derechos de las personas

El Estado protegerá y promoverá la protección de los derechos de las personas en Internet, a través del fortalecimiento de la institucionalidad existente en materia de ciberseguridad; y de la generación, adopción, y promoción de los mecanismos y las herramientas tecnológicas necesarias para que cada persona pueda integrarse a la sociedad y desarrollarse y expresarse plenamente.

03.
Cultura de ciberseguridad

Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas, responsabilidad en el manejo de tecnologías digitales, y promoción y garantía de los derechos de las personas.

04.
Coordinación nacional e internacional

El Estado **creará una gobernanza pública para coordinar las acciones necesarias en ciberseguridad.** Los organismos públicos y privados crearán, en conjunto, instancias de cooperación con el propósito de comunicar y difundir sus actividades en ciberseguridad, evitar la duplicación de trabajo y pérdida de recursos, y hacer eficientes los esfuerzos en esta área. En el ámbito internacional, **el Estado se coordinará con países, organismos, instituciones y otros actores internacionales** para permitir a nuestro país enfrentar de mejor manera las actividades maliciosas e incidentes en el ciberespacio.

05.
Fomento a la industria y la investigación científica:

El país promoverá el desarrollo de una industria de la ciberseguridad, que proteja a las personas y las organizaciones y que sirva a sus objetivos estratégicos. Para ello, fomentará la focalización de la investigación científica aplicada en temas de ciberseguridad, acorde a las necesidades del país.

La implementación de estos principios estratégicos permitirá a Chile enfrentar eficazmente los desafíos del ciberespacio. Con la colaboración público-privada y el respeto por los derechos de los ciudadanos, el país podrá crear un entorno digital seguro y resiliente, fomentando el desarrollo tecnológico y la innovación para un futuro próspero.

03. ¿A quiénes alcanza esta nueva ley de ciberseguridad?

La ley se aplica a instituciones del sector público y privado que se consideren prestadores de servicios esenciales y a aquellas designadas como operadores de importancia vital (OIV) por la ANCI.

Los servicios esenciales son aquellos servicios públicos realizados por organismos estatales o instituciones privadas, fundamentales para el normal funcionamiento del país.

Estas incluyen empresas dedicadas a:

- Generación y distribución de electricidad
- Banca y servicios financieros
- Telecomunicaciones
- Infraestructura digital y servicios digitales
- Servicios de tecnología de la información gestionados por terceros
- Suministro de agua potable y saneamiento
- Transporte terrestre, ferroviario, aéreo o marítimo
- Transporte, almacenamiento o distribución de combustibles
- Servicios postales y de mensajería
- Atención en salud, incluyendo hospitales y centros de producción de fármacos
- Administración de prestaciones de seguridad social

Por otro lado, los operadores de importancia vital (OIV) son prestadores de servicios esenciales que cumplen alguna de las siguientes características:

- Su servicio depende de redes y sistemas informáticos.
- La interrupción de su servicio tiene un impacto significativo en el orden público, la seguridad nacional o el cumplimiento de funciones del Estado.
- Su servicio debe ser garantizado por el Estado.

La ANCI puede designar a instituciones del sector privado como operadores de importancia vital si cumplen estas características, incluso si no son consideradas prestadores de servicios esenciales.

04. Prepara a tu empresa para cumplir con nueva Ley de Ciberseguridad en Chile

Con la implementación de esta nueva política nacional de ciberseguridad, las empresas deben ajustarse para cumplir con las nuevas normativas. Para ello, las instituciones implicadas deben tomar las siguientes acciones clave:

- ✓ Determinar si se califican como prestadores de servicios esenciales o como operadores de importancia vital.
- ✓ Comprender los aspectos de la ley y sus implicaciones en los procesos y objetivos empresariales.
- ✓ Evaluar su estado actual de cumplimiento y definir las acciones necesarias para optimizarlo.
- ✓ Alinear sus protocolos y políticas de seguridad informática con los requisitos de la ley.
- ✓ Capacitar a los empleados para que entiendan el alcance de la ley.

Estos pasos pueden servir como una base para que tu empresa desarrolle una estrategia de cumplimiento, protegiendo sus sistemas y redes informáticas y evitando sanciones.

En Babel, contamos con un equipo de expertos en ciberseguridad que puede adaptarse a las necesidades específicas de tu empresa para ayudarte a cumplir con las obligaciones de esta nueva ley.

Contacto

Correo: negocio.chile@babelgroup.com
Teléfono: +56 9 57583210

BABEL

babelgroup.com

IT CONSULTING. DIGITAL ACCELERATION. BUSINESS TRANSFORMATION.