**Ley Marco de Ciberseguridad (Ley N° 21.663)**

La Ley Marco de Ciberseguridad, publicada el 8 de abril de 2024, representa un hito fundamental para la protección de los activos digitales y la infraestructura crítica del país. Esta normativa establece un marco jurídico vinculante y transversal que obliga a instituciones públicas y privadas a adoptar medidas de seguridad informática, con el fin de prevenir, detectar, responder y recuperarse frente a incidentes cibernéticos.

**1. Objetivo central de la ley**

El objetivo de la Ley Marco de Ciberseguridad es fortalecer la resiliencia del ecosistema digital nacional mediante la creación de un sistema de gobernanza que regule:

* La prevención y gestión de riesgos cibernéticos.
* La coordinación público-privada frente a incidentes de ciberseguridad.
* El cumplimiento de obligaciones específicas por parte de entidades consideradas críticas para el funcionamiento del país.

**2. Ámbito de aplicación y sujetos obligados**

La ley distingue dos grandes categorías de entidades sujetas a obligaciones especiales:

* **Prestadores de Servicios Esenciales (PSE):** Empresas que operan en sectores clave para el funcionamiento de la sociedad y la economía, como transporte, energía, salud, telecomunicaciones, servicios financieros, agua potable, entre otros.
* **Operadores de Importancia Vital (OIV):** Infraestructuras cuya disrupción podría tener un impacto grave en la seguridad nacional, la salud pública o el orden económico. La clasificación como OIV es hecha por decreto fundado del Ministerio del Interior y Seguridad Pública, previo informe de la Agencia Nacional de Ciberseguridad (ANCI).

**3. Principales obligaciones para los Prestadores de Servicios Esenciales**

Las empresas consideradas PSE deben:

* **Adoptar medidas de ciberseguridad proporcionales** a los riesgos de sus operaciones.
* **Designar un encargado de ciberseguridad** con atribuciones claras.
* **Elaborar e implementar una política de ciberseguridad interna**.
* **Establecer y mantener un protocolo de reporte de incidentes cibernéticos**, que contemple los plazos definidos por reglamento.
* **Reportar incidentes relevantes a la ANCI** en plazos que van desde las 3 horas hasta los 15 días, dependiendo de la gravedad del evento.
* **Colaborar con la Agencia Nacional de Ciberseguridad (ANCI)** en procesos de investigación, mitigación y coordinación nacional.

Los **Operadores de Importancia Vital (OIV)**, además de cumplir con todas las obligaciones anteriores, tienen **exigencias adicionales más estrictas**, tales como:

* Contar con **certificación de cumplimiento de ciberseguridad** emitida por un tercero acreditado.
* Implementar **controles avanzados de seguridad** basados en estándares internacionales.
* Someterse a **auditorías periódicas obligatorias**.
* Tener definidos planes de continuidad operativa y recuperación ante desastres.
* Mantener **trazabilidad y conservación de evidencia digital** frente a incidentes graves.

**4. Rol de la Agencia Nacional de Ciberseguridad (ANCI)**

La ANCI es el ente rector del sistema nacional de ciberseguridad. Entre sus funciones están:

* Coordinar la respuesta ante incidentes de gran escala.
* Fiscalizar el cumplimiento de las obligaciones establecidas en la ley.
* Aplicar sanciones administrativas por incumplimientos.
* Emitir lineamientos, directrices técnicas y buenas prácticas.
* Gestionar el Registro Nacional de Prestadores de Servicios Esenciales.

**5. Reglamentos y plazos de cumplimiento**

La ley se complementa con varios reglamentos que regulan aspectos como:

* Los plazos y mecanismos de notificación de incidentes.
* Los criterios para la clasificación de entidades como OIV.
* Los requerimientos mínimos para las políticas de ciberseguridad.

Las empresas obligadas deben comenzar a implementar sus obligaciones dentro de los plazos definidos en dichos reglamentos, muchos de los cuales ya fueron publicados en 2025 y contemplan entre 6 y 12 meses de plazo para cumplimiento total.

**6. Consecuencias del incumplimiento y relevancia en el ámbito de Compliance**

El no cumplimiento de las obligaciones impuestas por la Ley Marco puede acarrear:

* **Multas administrativas significativas**, impuestas por la ANCI.
* **Responsabilidad penal de la persona jurídica**, si se configuran delitos informáticos o económicos en contexto de negligencia, conforme a la Ley 21.595 de Delitos Económicos.
* **Responsabilidad penal de directores y gerentes**, en caso de omisiones graves en la supervisión del cumplimiento legal.
* **Daño reputacional**, con consecuencias contractuales y de mercado.
* **Riesgos asegurables no cubiertos**, si no hay evidencia de cumplimiento normativo.

El cumplimiento de esta normativa es clave desde el enfoque de Compliance: refuerza la cultura organizacional, mejora la trazabilidad de decisiones, previene delitos y permite la defensa jurídica efectiva de la organización y sus líderes ante incidentes o investigaciones.

**7. Casos prácticos**

*Caso 1: Empresa de Transporte y Fraude Informático* Una empresa de transporte terrestre con operaciones logísticas digitales sufre una modificación maliciosa en su sistema de órdenes de despacho. Un supervisor, en complicidad con terceros, emite facturas falsas durante meses. La empresa no contaba con controles técnicos ni jurídicos adecuados. Como resultado, se le imputa responsabilidad penal por negligencia grave en prevención de delitos informáticos y económicos, conforme a la Ley 21.595.

*Caso 2: Empresa del Rubro de la Salud y Fuga de Datos* Una clínica privada, considerada prestadora de servicio esencial, sufre una brecha de seguridad por un ransomware que compromete datos clínicos sensibles de más de 10.000 pacientes. Se demuestra que no tenía políticas ni protocolos de ciberseguridad, ni capacitación a su personal. Además, se tardó más de 10 días en reportar el incidente a la ANCI, incumpliendo plazos legales. El hecho da lugar a sanciones, demandas civiles y exposición penal por infracción a la Ley 21.663 y a la Ley de Protección de Datos Personales.

**8. ¿Por qué una empresa que presta servicios esenciales debe cumplir con la Ley Marco de Ciberseguridad?**

**A. Porque la ley expresamente lo obliga.**

La Ley Marco de Ciberseguridad clasifica a los servicios esenciales, lo que implica que deben cumplir con las obligaciones específicas para ese tipo de operadores y en caso de incumplimiento se establecen sanciones.

**B. Porque una interrupción de los sistemas en este tipo de empresas puede afectar gravemente la continuidad operacional del país.**

En el sector transporte, los sistemas de logística, gestión de flotas, monitoreo satelital, control de accesos, y sistemas de despacho y trazabilidad son todos dependientes de tecnologías digitales. Un ciberataque puede:

* Detener el despacho de productos críticos (alimentos, combustibles, medicamentos).
* Afectar la cadena de suministro de supermercados, industrias o farmacias.
* Provocar congestión, accidentes o interrupciones masivas.
* Comprometer datos sensibles de usuarios, proveedores o trabajadores.

Ejemplo: un ransomware que afecte el sistema de control de flotas de una empresa de logística masiva podría impedir que lleguen productos a más de 200 supermercados en menos de 24 horas.

Lo mismo sucede en otros rubros como la salud, la generación de energía y el sector financiero, un ciberataque a un eslabón de la cadena de suministros en todos estos servicios esenciales puede generar un efecto importante para la economía del país e incluso para la salud de las personas.

**C. Porque el incumplimiento puede generar sanciones, responsabilidad penal y daño reputacional**

No cumplir con las obligaciones de la ley puede tener consecuencias graves:

* Sanciones administrativas impuestas por la Agencia Nacional de Ciberseguridad (ANCI), que van desde amonestaciones hasta multas económicas.
* Responsabilidad penal por delitos informáticos (Ley 21.459) si hay negligencia grave que facilita ataques.
* Responsabilidad penal de la persona jurídica si el incidente deriva en delitos que afecten a terceros, de acuerdo con la Ley N° 21.595 de Delitos Económicos.
* Daño reputacional y pérdida de contratos (por ejemplo, con grandes retailers o instituciones públicas que exigen cumplimiento normativo).
* Riesgo de ser demandada por terceros afectados (por ejemplo, por incumplimiento contractual si no entregan productos a tiempo debido a una falla cibernética).

**D. Porque debe colaborar con la ANCI y reportar incidentes**

Una empresa no puede actuar sola frente a un ciberataque. La ley la obliga a:

* Designar un encargado de ciberseguridad que será interlocutor con la ANCI.
* Reportar incidentes relevantes en plazos breves (3h, 72h, 7 días, etc.) según su impacto.
* Implementar protocolos, políticas y controles de seguridad alineados con los estándares nacionales.
* Colaborar con el CSIRT nacional y otros actores del ecosistema en caso de crisis.

**E. Porque la ciberseguridad es un factor estratégico en contratos, licitaciones y asegurabilidad**

Hoy, muchas grandes empresas o instituciones públicas exigen evidencia de cumplimiento en ciberseguridad como condición para contratar o renovar contratos.

Además:

* Las aseguradoras ciber no otorgan cobertura si la empresa no tiene modelos mínimos de cumplimiento.
* La CMF y la Ley de Delitos Económicos pueden cruzar información con la ANCI si hay vulneración de sistemas financieros o afectación económica grave.

**Conclusión**

La Ley Marco de Ciberseguridad representa un cambio de paradigma: ya no basta con soluciones técnicas, sino que se requiere una **gobernanza jurídica** de la ciberseguridad. Su implementación adecuada requiere la participación activa de equipos legales, técnicos y de alta dirección. Es, al mismo tiempo, una obligación legal y una oportunidad para fortalecer la competitividad, la sostenibilidad y la protección integral de las empresas chilenas.