KPMG Webcast: Temas Imprescindibles | Voces Expertas

Ciberseguridad e Infraestructura Crítica de Información

¿Esta su organización preparada para cumplir con la ley marco y proteger sus infraestructuras criticas antes las crecientes amenazas digitales?

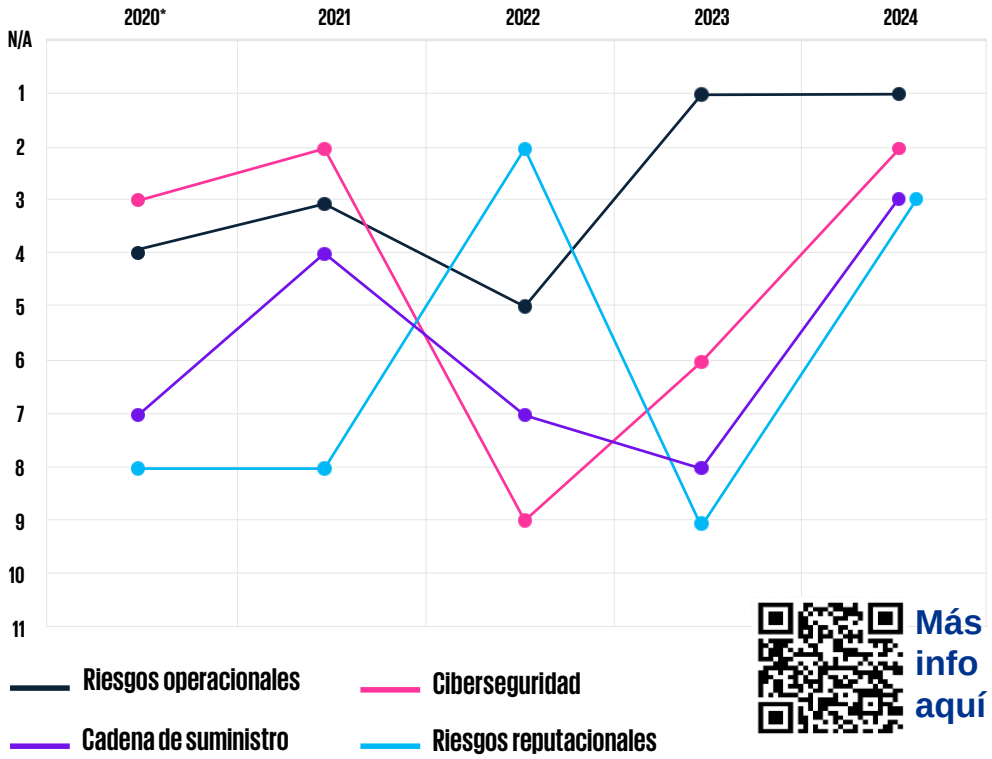
Advisory – Consulting

Febrero 2025

La ciberseguridad ha escalado posiciones entre las principales preocupaciones para las compañías:

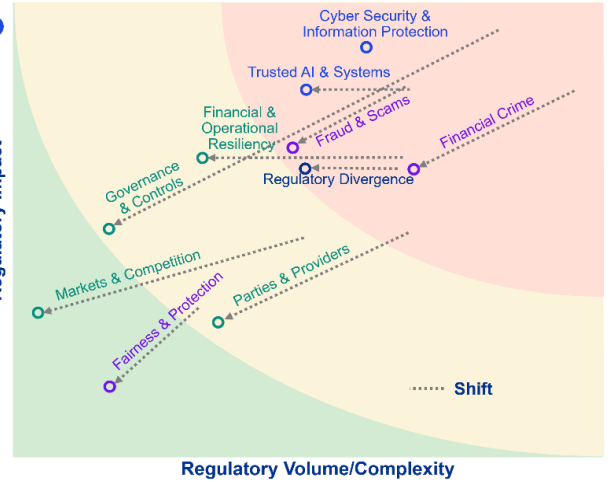
Evolución en los últimos diez años de los principales riesgos para el crecimiento identificados en 2024

Puesto definido en base al porcentaje de respuesta registrado por cada una de estas opciones en las distintas ediciones

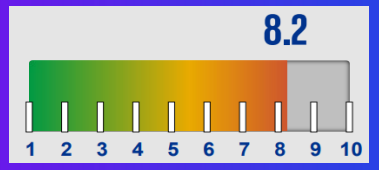


Más info aquí

2025 Año del cambio regulatorio



Ciberseguridad y Protección de Datos
Barómetro Regulatorio



Más info aquí

Dado que los riesgos en ciberseguridad siguen siendo una preocupación clave en todas las industrias, y en particular en relación con la seguridad y las infraestructuras críticas, el escrutinio normativo de la seguridad de los datos, la gestión del riesgo de los datos, la resiliencia operativa y la notificación/respuesta ante incidentes continuará en la agenda 2025.

Objetivo:

Establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre estos y los particulares

Además, busca establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad, así como definir las atribuciones y obligaciones de los organismos del Estado, los **deberes de las instituciones determinadas** y los mecanismos de control, supervisión y responsabilidad ante infracciones.

Concretamente, la creación de la **ANCI - Agencia Nacional de Ciberseguridad es neurálgica** para centralizar la estrategia de ciberseguridad del país, coordinar las acciones entre diferentes entidades y supervisar la implementación de la política nacional en materia de ciberseguridad.

Esta ley es vinculante. Esto significa que las disposiciones contenidas en la ley son de obligatorio cumplimiento para las entidades y organizaciones a las que se aplica.

La **ANCI** también busca promover un entorno digital más seguro y confiable para todos los ciudadanos, siendo la punta de lanza en las maniobras del estado en estas materias.

La estrategia del Estado chileno detrás de la Ley Marco de Ciberseguridad se centra en varios **aspectos fundamentales para mejorar la seguridad del espacio cibernético nacional**, lo cual incluye: estructuración y regulación, prevención de ciberincidentes, respuesta y mitigación, colaboración sectorial, protección de infraestructuras criticas, capacitación y concientización, marco legal y sanciones, además de adaptabilidad y actualización continua.

Varios países alrededor del mundo han implementado leyes de ciberseguridad para proteger sus infraestructuras críticas y asegurar sus activos de información en un entorno digital:

USA - (Cybersecurity Information Sharing Act) de 2015.

Europa - Network and Information Security) de 2016.

Australia - Ley de Seguridad de la Infraestructura Crítica (2020).

Japón - Ley de Ciberseguridad Básica (2014).

UK - Ley de Seguridad de la Red y Sistemas de Información (NIS Regulations 2018)

Unión Europea - NIS 2 (2023)

Ante lo cual surgen interrogantes, que esclarecemos a continuación:

1. ¿Cuándo se darán a conocer los reglamentos y clasificación de empresas?

Según la fecha de promulgación de la ley 12 de Diciembre de 2024, se estipula que dentro del plazo **de ciento ochenta días posteriores a la publicación de la ley**, el Ministerio del Interior y Seguridad Pública debe expedir los reglamentos señalados en la ley. Estos reglamentos son esenciales para especificar detalles, procedimientos y mecanismos de implementación y cumplimiento de la ley, cubriendo aspectos técnicos y administrativos para facilitar la aplicación efectiva de la Ley Marco de Ciberseguridad. Los reglamentos jugarán un papel clave en precisar roles, responsabilidades y procedimientos que han sido delineados de forma general en la ley.

La ley establece que la Agencia Nacional de Ciberseguridad (ANCI) tiene la responsabilidad de identificar y clasificar las instituciones que presten servicios esenciales y aquellas que sean calificadas como operadores de importancia vital.

Sin embargo, **el texto legal no especifica una fecha exacta** para la publicación final de esta lista de empresas consideradas como servicios esenciales o operadores de importancia vital. Es razonable suponer que durante el primer año de implementación de la ley, se trabajará intensivamente en la catalogación y publicación de estas listas, tomando en cuenta los tiempos administrativos y de consulta pública requeridos para tal efecto.

Dado el contexto y propósito de la Ley Marco de Ciberseguridad, es probable que ciertos sectores críticos sean priorizados en la clasificación como servicios esenciales y operadores de importancia vital debido a su alto impacto en la seguridad, economía y bienestar social.

Consideramos que los siguientes sectores pueden ser priorizados dentro de la catalogación:

- **SALUD** - Hospitales y clínicas, Laboratorios y centros de investigación biomédica. Sistemas de gestión de emergencias y respuesta sanitaria.
- **Telecomunicaciones y TI** - ISP, infraestructura de red y centros de datos, servicios de TI y plataformas digitales esenciales.
- **Energía y Servicios Públicos** - Generación, transmisión y distribución eléctrica. Plantas de tratamiento y distribución de agua potable. Gestión de residuos y servicios de saneamiento.
- **Finanzas** - Bancos e instituciones financieras. Bolsas de valores. Sistemas de pago y liquidación.
- **Seguridad Nacional y Orden Público** - Fuerzas armadas y de orden. Inteligencia y servicios de respuesta a emergencias y desastres.
- **Manejo de Recursos Naturales** - Minería y explotación de recursos naturales clave. Productos químicos y materiales peligrosos.
- **Transporte** - Transporte aéreo, terrestre, marítimo y ferroviario. Infraestructura asociada fundamental para la operación y gestión del tráfico y transporte.
- **Gobierno y Administración Pública** - defensa y seguridad nacional, sistemas de gestión de registros públicos y datos personales.

2. ¿Qué podemos anticipar durante este semestre?

Durante los 180 días en que se están elaborando y finalizando los reglamentos bajo la Ley Marco de Ciberseguridad, **las empresas pueden tomar varias medidas proactivas para prepararse adecuadamente y ganar tiempo** una vez que la ley entra en vigencia completamente. Aquí hay algunos pasos clave que las empresas pueden considerar:

Las propias organizaciones serán responsables de analizar y determinar que focos plantear de manera proactiva para fortalecer su postura de ciberseguridad, previo a la llegada de los reglamentos y catálogos.

Al tomar estos pasos, las empresas no solo estarán mejor preparadas para cumplir con la nueva ley una vez que los reglamentos sean publicados, sino que también **fortalecerán su postura general de ciberseguridad frente a amenazas emergentes**, beneficiando su operatividad y reputación a largo plazo.

Consideraciones Proactivas
Muchas organizaciones están optando por autoevaluarse bajo el paraguas de máxima, **Servicio Esencial**
Evaluación técnica de ciberseguridad y comparación con prácticas y estándares internacionales.
Concientización y capacitación para empleados y clientes.
Expandir la evaluación incorporando consultoría legal y de cumplimiento.
Ampliar la inversión e infringir mejoras en la tecnología de sus ecosistemas.
Desarrollo de planes de respuesta a incidentes basados en un perfil de amenazas realista.
Dialogo abierto con gremios y partes interesadas para compartir enfoques y aplicabilidad.
Revisión de contratos con proveedores de servicios para proteger la cadena de suministros.
Fortalecer la clasificación de activos de información y soporte.
Fortalecer Gestión de riesgos de tecnología, ciberseguridad y seguridad de la información.
Fortalecer la resiliencia y continuidad de negocios (esto incluye BIA y RIA).

No definimos prioridades…

Este grupo de consideraciones proactivas, ya vienen siendo abordadas por mucho de nuestros clientes, siendo especialmente preponderantes las resaltadas en negrita, pues han sido los focos en sectores regulados y no regulados.

Estos criterios han sido definidos en función de nuestra lectura del mercado local.

3. ¿Cuan exigentes son las medidas de supervisión para las empresas alcanzadas por la ley?

Para clarificar y distinguir las medidas de supervisión aplicables por la Agencia Nacional de Ciberseguridad (ANCI) tanto para operadores de importancia vital como para servicios esenciales, es útil organizar la información en una tabla. Aquí presentamos una comparativa de las responsabilidades y obligaciones que deben cumplir estas entidades bajo la supervisión de la ANCI:

Criterio / Categoría	Servicios Esenciales - Medidas de supervisión por parte de la autoridad:	Operadores de importancia vital – Medidas de supervisión menos exigentes:
Auditorias de Seguridad	Auditorías regulares para asegurar el cumplimiento normativo.	Auditorías periódicas para identificar riesgos y vulnerabilidades.
Reporte de Incidentes	Reporte obligatorio de incidentes, especialmente los que impactan la continuidad del servicio.	Reporte obligatorio de incidentes de ciberseguridad a la ANCI.
Planes de Continuidad	Requerimiento similar de mantener planes de continuidad operacional robustos.	Desarrollar e implementar planes de continuidad operacional y ciberseguridad
Certificaciones	Necesidad de cumplir con estándares y posiblemente obtener certificaciones relevantes.	Posible requerimiento de obtener certificaciones de seguridad específicas.
Formación y capacitación	Capacitación obligatoria para el personal en prácticas de ciberseguridad.	Adherencia a los estándares nacionales e internacionales de ciberseguridad.
Cumplimiento de estándares	Similar adherencia a los estándares establecidos por la ANCI y otros organismos.	Programas continuos de formación en ciberseguridad para el personal.
Fiscalizaciones e inspecciones	Inspecciones para asegurar la integridad y seguridad de las operaciones críticas.	Inspecciones regulares por parte de la ANCI para verificar el cumplimiento.
Cooperación intergubernamental	Similar requerimiento de participar en iniciativas de cooperación para mejorar la respuesta a incidentes.	Deben participar en redes de intercambio de información de amenazas.

4. ¿Cómo podemos ayudarles desde KPMG?

La ley presenta varios desafíos y requerimientos para las empresas, especialmente aquellas identificadas como operadores de importancia vital o proveedores de servicios esenciales. A continuación, damos a conocer cómo los servicios de ciberseguridad de KPMG pueden alinearse y satisfacer las necesidades específicas de nuestros clientes:

Nuestro portfolio de soluciones ciberseguridad y de privacidad

- Estrategia, gobernanza, riesgo y cumplimiento
- Programas de mejora transformacionales de ciberseguridad
- Servicios de gestión, respuesta y recuperación de amenazas
- Servicios gestionados de ciberseguridad
- Resiliencia y continuidad del negocio
- Potección de distintos ecosistemas
  - Personas
  - Datos
  - Cadena de Suministros
  - Plataformas
  - Productos
  - Tecnologíoa Operacional
  - Tecnologías Disruptivas
- Evaluaciones de ciberseguridad y privacidad de datos personales

Alianzas

Microsoft, aws, Google Cloud, CLAROTY, grclinks, RSA, servicenow, RELIAQUEST, CYBERARK, SailPoint, okta, OneTrust, CYLANCE, securiti

Contáctanos

En el entorno actual, la confianza es la base sobre la que vertebrar la ciberseguridad.

Desde KPMG, nuestra misión y nuestro foco se centran en ofrecer a nuestros clientes **las mejores soluciones y enfoques para su realidad**, ya venga marcada por imperativo interno, por regulaciones (locales, globales o sectoriales) o fruto de sus procesos de transformación digital.

Erick Palencia

Socio Consulting y Líder en Ciberseguridad
KPMG en Chile.
E: erickpalencia@kpmg.com
T: +56959910502

Juan José Hernández

Director Consulting y Ciberseguridad
KPMG en Chile.
E:juanjhernandez@kpmg.com
T:+56966074535

La ciberseguridad, la privacidad y la protección de la información, sea cual sea el perímetro de trabajo, se presentan como **pilares de confianza** para un negocio que, fruto de la recolección y analítica de datos, la cada vez mayor dependencia tecnológica o el aumento de vectores de exposición, **necesita evolucionar y recorrer este proceso con garantías**, de manera estratégica y transversal a toda la compañía.

Te ayudamos a adaptarte a las nuevas legislaciones en materia de ciberseguridad y protección de datos personales

Descubre cómo

Ciberseguridad e Infraestructura Crítica de Información

kpmg.com/cl

KPMG en Chile


KPMG