COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Rol de la CMF en los desafíos de ciberseguridad y protección de datos

Catherine Tornel L.
Presidenta
Comisión para el Mercado Financiero
Abril 2026

Riesgos tecnológicos en la economía global

- El Foro Económico Mundial incluye continuamente los riesgos de tecnología, manejo de información y ciberseguridad dentro de los de mayor severidad a nivel global para el corto y largo plazo.

WEF 2026

N°	Corto plazo	Largo plazo
1	Confrontación geoeconómica	Eventos climáticos extremos
2	**Desinformación y mala información**	Pérdida de biodiversidad y colapso de ecosistemas
3	Polarización social	Cambios críticos en los sistemas de la Tierra
4	Eventos climáticos extremos	**Desinformación y mala información**
5	Conflicto armado entre Estados	**Consecuencias adversas de las tecnologías de IA**
6	**Inseguridad cibernética**	Escasez de recursos naturales

WEF 2025

N°	Corto plazo	Largo plazo
1	**Desinformación y mala información**	Eventos climáticos extremos
2	Eventos climáticos extremos	Pérdida de biodiversidad y colapso de ecosistemas
3	Conflicto armado entre Estados	Cambios críticos en los sistemas de la Tierra
4	Polarización social	Escasez de recursos naturales
5	**Ciberespionaje y guerra cibernética**	**Desinformación y mala información**
6	Contaminación	**Consecuencias adversas de las tecnologías de IA**

La exposición a este riesgo es transversal a los agentes del entorno digital (personas, empresas, estados)

Los nuevos métodos de ciberataques que llegarán a Latinoamérica en 2026

Expertos proyectan los primeros ataques articulados completamente con IA, la clonación de tarjetas con tecnología inalámbrica y espionaje con computación cuántica.

OpenAI warns new models pose 'high' cybersecurity risk

By **Reuters**

December 10, 2025 7:54 PM GMT-3 · Updated December 10, 2025

CIBERSEGURIDAD

Ciberseguridad: 2026 expertos pronostican mayores ciberamenazas financieras impulsadas por IA y un auge de fraudes dirigidos a pagos móviles

El secretario del Tesoro Bessent y el presidente de la Fed Powell se reúnen con directores ejecutivos de bancos sobre riesgos de IA de Anthropic

Por Investing.com | Editor Ambar Warrick | Bolsa

Publicado 10.04.2026, 06:07

Office of the Comptroller of the Currency

Home > News & Events > Newsroom

News Release 2025-30 | April 8, 2025

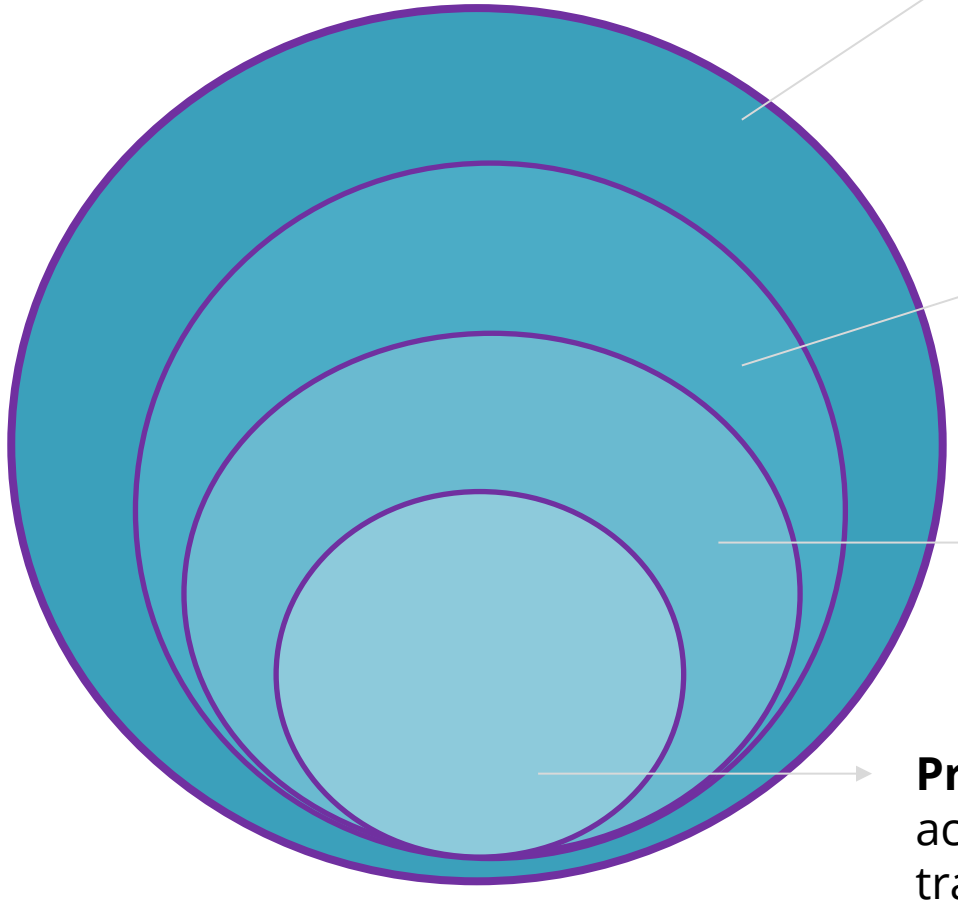
OCC Notifies Congress of Incident Involving Email System

18/07/2025

Brasil sufre el mayor ciberataque financiero de su historia bancaria

La venta de credenciales de cuenta privilegiada permitió a ciberdelincuentes transferir fondos del Banco Central brasileño a cuentas en el extranjero y convertirlos en criptomonedas.

Existe una relación entre los componentes de ciberseguridad, gestión de datos y privacidad a partir del riesgo operacional



Gestión del riesgo operacional: prácticas y políticas para mitigar pérdidas o disrupciones derivadas de fallas en procesos, personas, sistemas o eventos externos, que pueden afectar la continuidad de los servicios financieros y, potencialmente, la estabilidad del sistema.

Ciberseguridad: protección ante pérdida, alteración, indisponibilidad o acceso no autorizado a sistemas o información que afecta la integridad, confidencialidad y disponibilidad del servicio.

Gobernanza de datos: Políticas, estructuras y controles que aseguran que los datos sean gestionados de manera segura, íntegra, trazable y conforme a su finalidad.

Privacidad de datos: Protección de los datos personales frente a accesos, usos o divulgaciones no autorizadas, asegurando que su tratamiento se realice conforme al marco legal y los derechos de los titulares de los datos.

Ciberseguridad y protección de datos personales en el servicio financiero moderno

Servicio financiero moderno

- **Digitalización y complejidad tecnológica**: Interoperabilidad de los sistemas, dependencia de infraestructura *cloud*, coexistencia de sistemas "*legacy*" con tecnologías modernas, procesos críticos completamente digitalizados.
- **Nuevos modelos de negocio**: Servicios Fintec, Finanzas Abiertas, banca digital, plataformas de intermediación, externalización de funciones críticas, Software as a Service (SaaS), nuevas interfaces en los servicios finales.
- **Riesgos derivados y amenazas emergentes**: Concentración en proveedores tecnológicos, dependencias ocultas en la cadena de valor (cuartas partes), ciberataques, amenazas persistentes avanzadas (APT), exfiltración masiva de datos, otros.
- **Desafíos de gestión interna**: Tratamiento de datos sensibles, continuidad operacional, exigencias de trazabilidad, brechas de talento especialista, dificultad de integración entre áreas (riesgo – TI – negocio).

Requiere balance entre:

Eficiencias operacionales y adecuada gestión a mayores riesgos de ciberseguridad y de tratamiento de información sensible.

Nuevas prioridades regulatorias a nivel global en ciberseguridad, datos y riesgo tecnológico

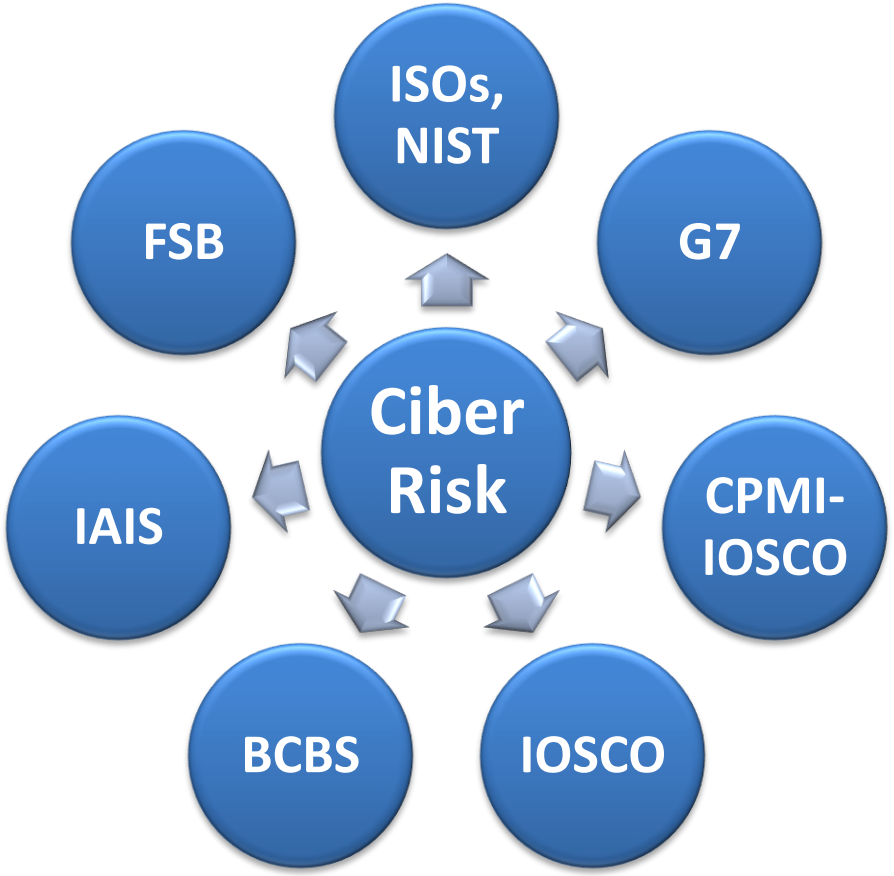
- La literatura reciente de BIS, FSB, IMF y EBA muestra que la digitalización financiera ha puesto en la agenda regulatoria los riesgos de **ciberseguridad, tecnología y protección de datos**.

- El interés supervisor se ha desplazado desde el cumplimiento de estándares generales de riesgo operacional hacia la evaluación de materias específicas: **gobernanza de datos, resiliencia operacional, riesgo de terceros y capacidad de respuesta sistémica.**

Datos → Un nuevo eje para regular y supervisar	Digitalización → mayor exposición al riesgo	Ciberseguridad → riesgo estratégico	Enfoque en su efecto sistémico
• El uso intensivo de datos (incluidos personales) eleva la relevancia de la privacidad, gobernanza y control en el sector financiero.	• Creciente dependencia de tecnología, datos y proveedores amplía la exposición a riesgos operacionales y de información.	• Deja de ser un tema técnico y pasa a ser un problema de resiliencia operacional y estabilidad financiera.	• Existen riesgos y asuntos interconectados: terceros, proveedores críticos y coordinación entre autoridades.

El riesgo cibernético representa un desafío para la estabilidad y la confianza en los mercados financieros

Para abordar estos desafíos, diferentes organismos internacionales han desarrollado estándares y lineamientos regulatorios.

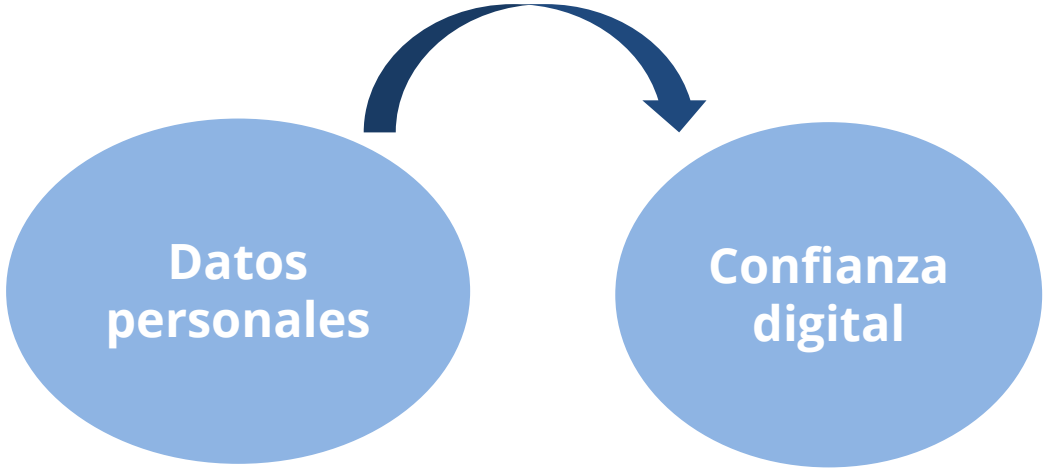


DORA
NIS 2
TIBER-EU

Lineamientos de supervisión y regulación CBEST

Protección de datos personales como pilar adicional de confianza digital en el sistema financiero

La transformación digital de los servicios financieros intensifica el uso de datos personales, sensibles, transaccionales y conductuales. Por ello, distintas jurisdicciones han reforzado sus marcos legales para asegurar licitud, transparencia, control del titular, seguridad y responsabilidad en el tratamiento de datos.



GDPR

Data Protection Act 2018

LGPD

CALIFORNIA PRIVACY RIGHTS ACT

Panorama general de la Ciberseguridad y protección de datos personales en Chile

- La actuación de la CMF en ciberseguridad y protección de datos personales se desarrolla dentro de un marco legal cada vez más robusto y amplio:

Marco nacional transversal

- Política Nacional de Ciberseguridad.
- Ley de protección de datos personales.
- Ley de fraude.
- Ley de delitos informáticos.

Marco específico CMF

- Leyes de bancos y cooperativas.
- Ley de seguros.
- Leyes de mercado de valores, fondos, sociedades e infraestructuras.

Cambios recientes

- Ley marco de ciberseguridad.
- Actualización a la Ley de Protección de Datos Personales.
- Cambio en la Ley de Fraudes.
- Ley Fintech.

Disposiciones normativas generales

- Exigencias de Gobierno Corporativo y gestión de riesgos.
- Gestión de incidentes.
- Enfoque proporcional.

Ciberseguridad y protección de datos personales en torno a los mandatos de la Comisión para el Mercado Financiero

- La CMF tiene la misión de velar por el correcto funcionamiento, desarrollo y estabilidad del mercado financiero, facilitando la participación y promoviendo el cuidado de la fe pública.

- El funcionamiento actual de los mercados se realiza en torno a una transformación digital y exposición a nuevos riesgos. Lo anterior incide en los tres mandatos de la CMF:

	¿Por qué?	Un incidente grave…
Prudencial	Vinculada a los ámbitos de continuidad de negocios, de seguridad la información, de proveedores y de tecnología, los que se vinculan con procesos críticos (cadena de pagos, compensación, liquidación, etc.)	Puede transformarse en un evento de estabilidad financiera.
Conducta de Mercado	Afecta a la privacidad de los usuarios y al derecho de que su información esté resguardada, especialmente considerando datos sensibles.	Atenta contra la protección del cliente, sus datos y su desenvolvimiento en el mercado financiero.
Desarrollo de mercado	La seguridad en el entorno digital es una condición para el crecimiento y sano funcionamiento de los mercados.	Ralentiza la adopción de productos modernos y genera tensiones para la innovación (usuarios y oferentes).

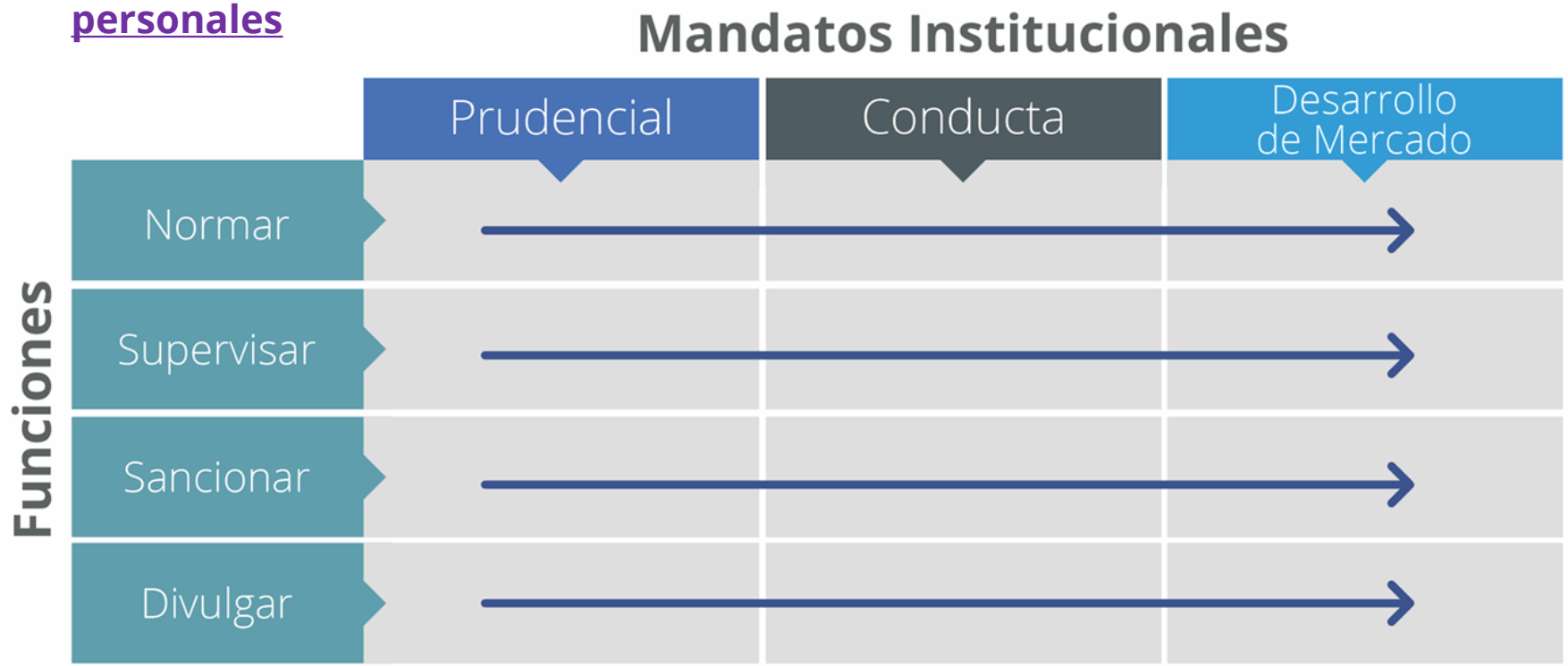
Ciberseguridad y protección de datos personales en torno a las funciones de la Comisión para el Mercado Financiero

Ciberseguridad y protección de datos personales

Potencial impacto sistémico

Incidencia en la protección al cliente

Efecto en la confianza en el sistema



Fuente: CMF.

Curso de acción:

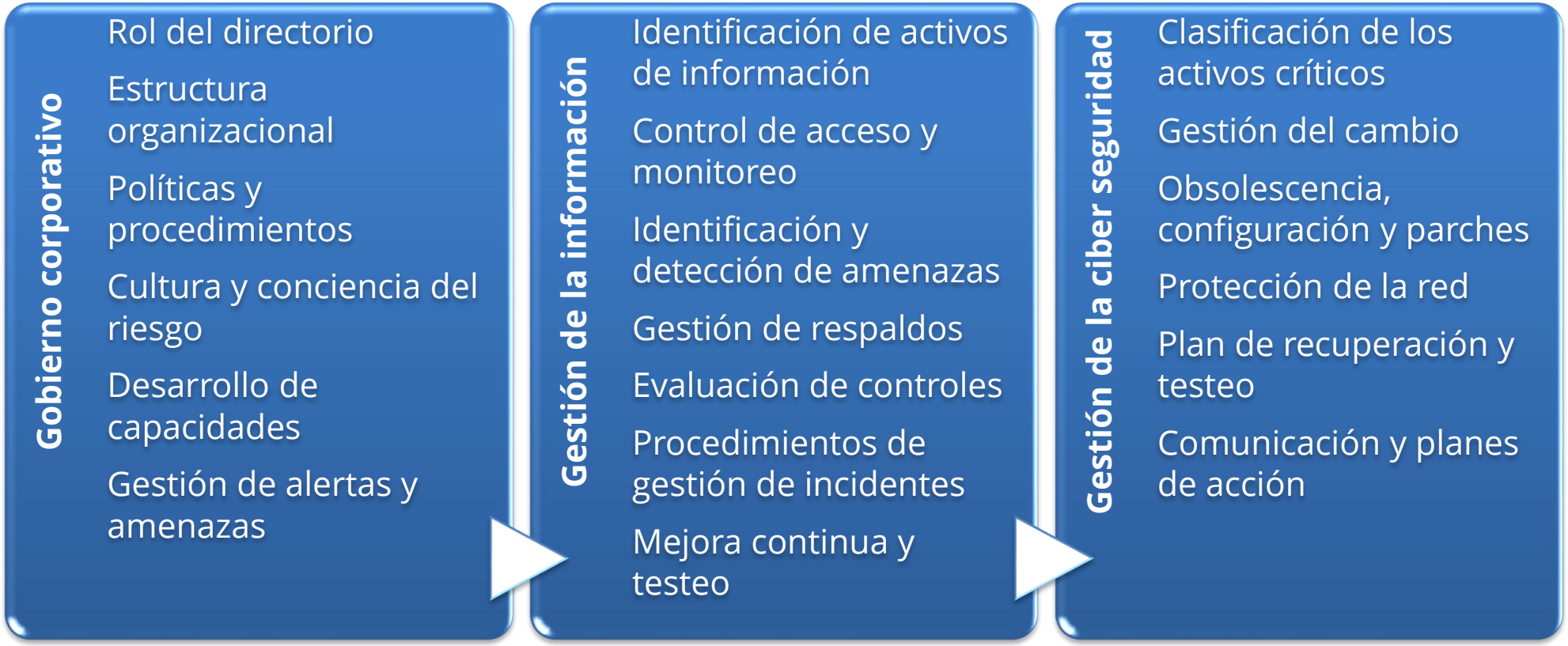
Definir estándares para promover un mejor nivel esperado de seguridad (ej. NCG 510, RAN Capítulos 20-7 a 20-10 y otros).

Fiscalizar la implementación, evaluando cumplimiento, madurez, reportes y calidad de la gobernanza.

Actuar cuando hay incumplimientos, fallas graves o afectación a clientes.

Coordinar entre fiscalizados y otras agencias, comunicar públicamente en caso de ser necesario e incluir esta materia en reportes anuales.

Ciberseguridad y protección de datos personales en torno a las funciones de regulación y supervisión de la CMF



Nuestra regulación fomenta (1) el intercambio de información sobre incidentes cibernéticos en toda la industria financiera, (2) el seguimiento del curso de acción e implicancias y (3) la exigencia de adoptar medidas ante tales instancias.

La situación del riesgo de ciberseguridad y protección de datos personales permite revisitar paradigmas de la industria

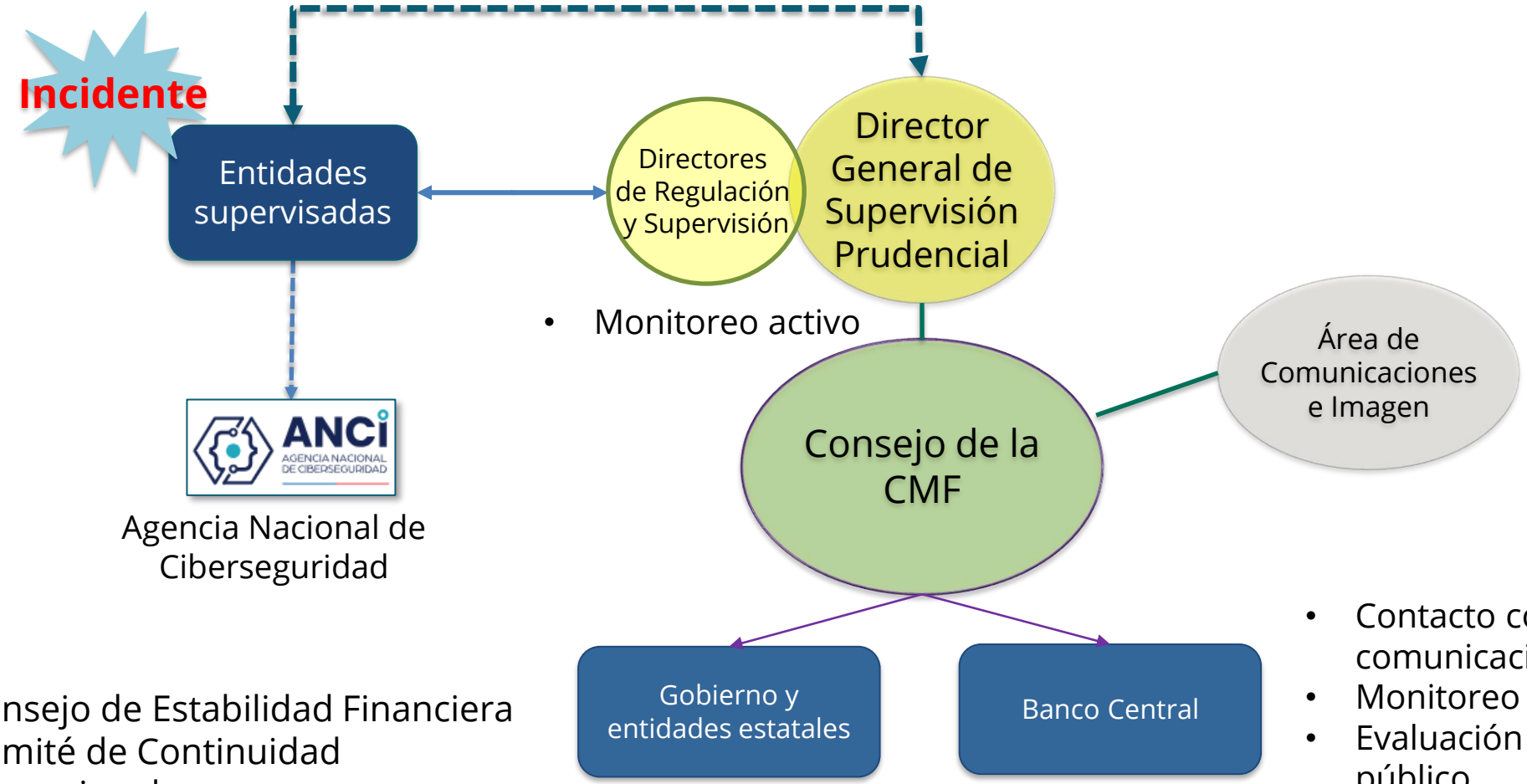
No es sólo función preventiva, sino por la capacidad contenerlos sin afectar funciones críticas.

El cumplimiento normativo es una línea de base, ya que la gestión de riesgos debe apuntar a gestionar este riesgo en un entorno cambiante y dinámico.

Cuando la operación depende estructuralmente de la tecnología, TI deja de ser soporte y pasa a ser una dimensión estratégica del negocio.

En un sistema financiero interconectado, un incidente cibernético puede dejar de ser un problema individual y transformarse en un problema sistémico.

Existe un enfoque de la coordinación interinstitucional ante incidentes



- Consejo de Estabilidad Financiera
- Comité de Continuidad Operacional

- Contacto con medios de comunicación.
- Monitoreo de redes sociales.
- Evaluación de información al público.

La regulación de la CMF aborda diferentes temáticas en esta materia, las cuales están en continua revisión:

Bancos: Capítulos 20-7 al 20-7 de la RAN de bancos

Infraestructuras y actores de industria de valores: NCG N°510

Aseguradoras y reaseguradoras: NCG N°454

Servicios Fintec: NCG N°502

Reportantes del REDEC: NCG N°540

Existen espacios para la innovación en estas materias

- La CMF ha tendido a especificar exigencias generales a mecanismos trazables y verificables en materia de ciberseguridad y protección de datos. No basta declarar o incluir en una política la existencia de un control, sino que haya evidencia técnica, responsabilidad y capacidad de verificación.

- Dos casos relevantes y recientes al respecto que estuvieron en consulta pública:

Hash y gestión del consentimiento (REDEC)
→ El dato deja de ser "declarado" y pasará a ser comprobable.

Terceras partes y cuartas partes en externalización (Bancos, Capítulo 20-7 RAN).
→ El servicio externalizado pasará a ser más gestionable y controlable por el cliente.

Conclusiones y desafíos futuros para la industria financiera

- A pesar de los avances en institucionalidad y buenas prácticas de la industria, los riesgos cibernéticos representan un creciente desafío para el sector financiero y son de gestión prioritaria.

- Los requisitos actuales y futuros son materia en constante revisión y relacionadas al Plan de Regulación de la CMF, especialmente por el surgimiento de nuevos riesgos no financieros.

- La experiencia ha demostrado que la cooperación y la comunicación interinstitucional son fundamentales para una gestión eficaz de incidentes. En la actualidad, la CMF se encuentra desarrollando coordinaciones con la ANCI y avanzando en los preparativos para articularse con la futura Agencia de Protección de Datos Personales con el fin de limitar daños y ejercer atribuciones rápidamente cuando se produzca un incidente de ciberseguridad.

- La CMF tiene un rol proactivo y prospectivo para tomar medidas regulatorias, de supervisión y de coordinación oportunas en pro de la ciberseguridad, la protección de datos y la privacidad de la información.

COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Rol de la CMF en los desafíos de ciberseguridad y protección de datos

Catherine Tornel L.
Presidenta
Comisión para el Mercado Financiero
Abril 2026