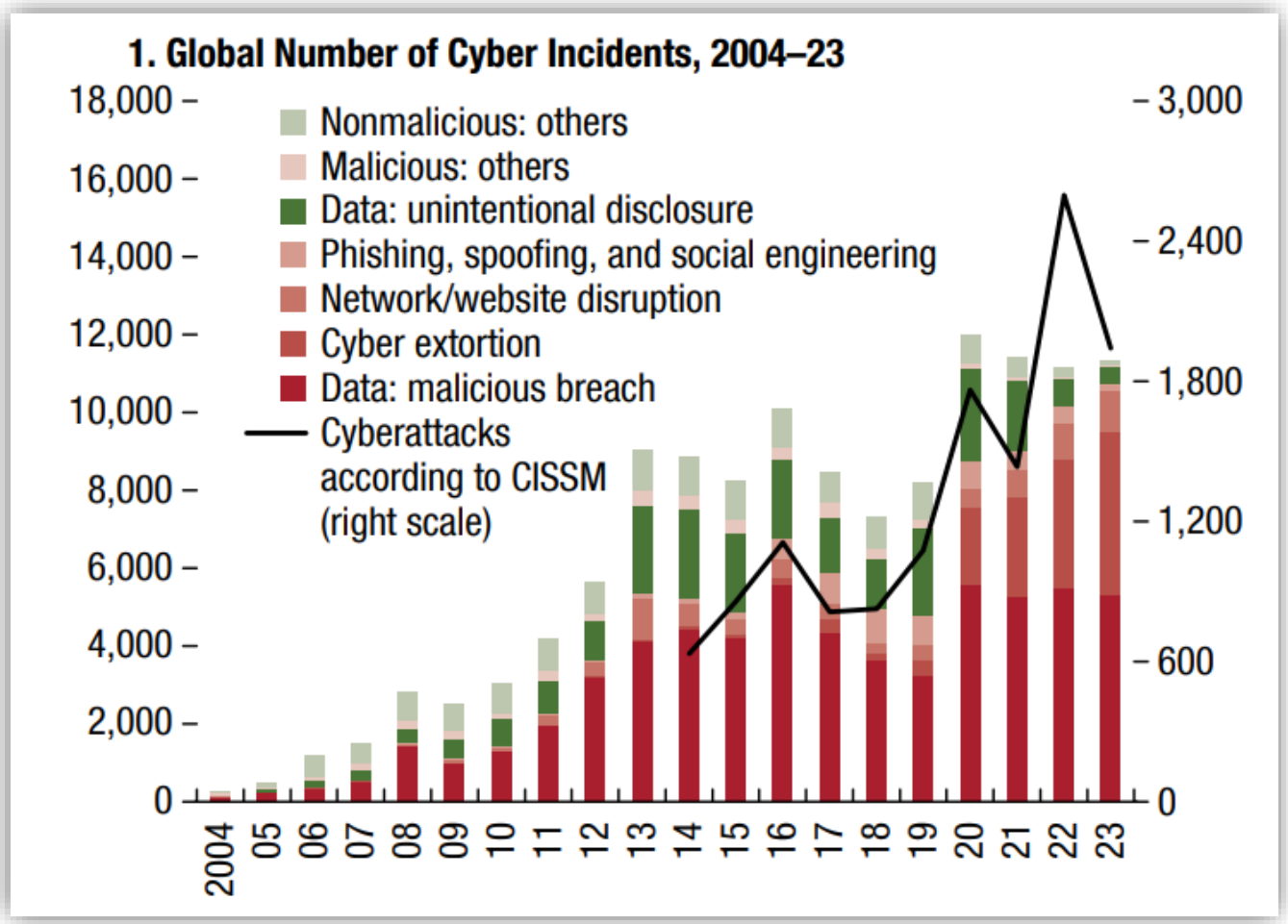
100 años de regulación y supervisión bancaria

COMISIÓN PARA EL MERCADO FINANCIERO

Ciberseguridad: La experiencia de la CMF

Francisco Cabezón Ferraté
Director General de Regulación Prudencial
24 de Octubre de 2025

El riesgo cibernético se ha convertido en parte de nuestra vida cotidiana



Fuente: FMI (2024)

El número de incidentes cibernéticos, especialmente los de naturaleza maliciosa, ha aumentado drásticamente en las últimas dos décadas (WEF, 2024).

No podemos controlar cuántos ataques se intentan, pero sí podemos implementar controles para evitar o mitigar su impacto y, por supuesto, gestionar la respuesta ante incidentes y la recuperación.

La industria financiera es uno de los principales objetivos de los ciberataques

BANGLADESH SAYS HACKERS STOLE $100 MILLION FROM ITS US FEDERAL RESERVE ACCOUNT

Pierluigi Paganini March 09, 2016

securityaffairs

CNBC MARKETS BUSINESS INVESTING TECH POLITICS VIDEO INVESTING CLUB JOIN PRO JOIN

China's ICBC, the world's biggest bank, hit by cyberattack that reportedly disrupted Treasury markets

PUBLISHED FRI, NOV 10 2023·6:15 AM EST | UPDATED FRI, NOV 10 2023·10:21 AM EST

Reuters World Business Markets Sustainability More

Bank of Chile trading down after hackers rob millions in cyberattack

By **Reuters**

June 11, 2018 7:47 PM GMT-4 · Updated June 11, 2018

FINTECH FUTURES

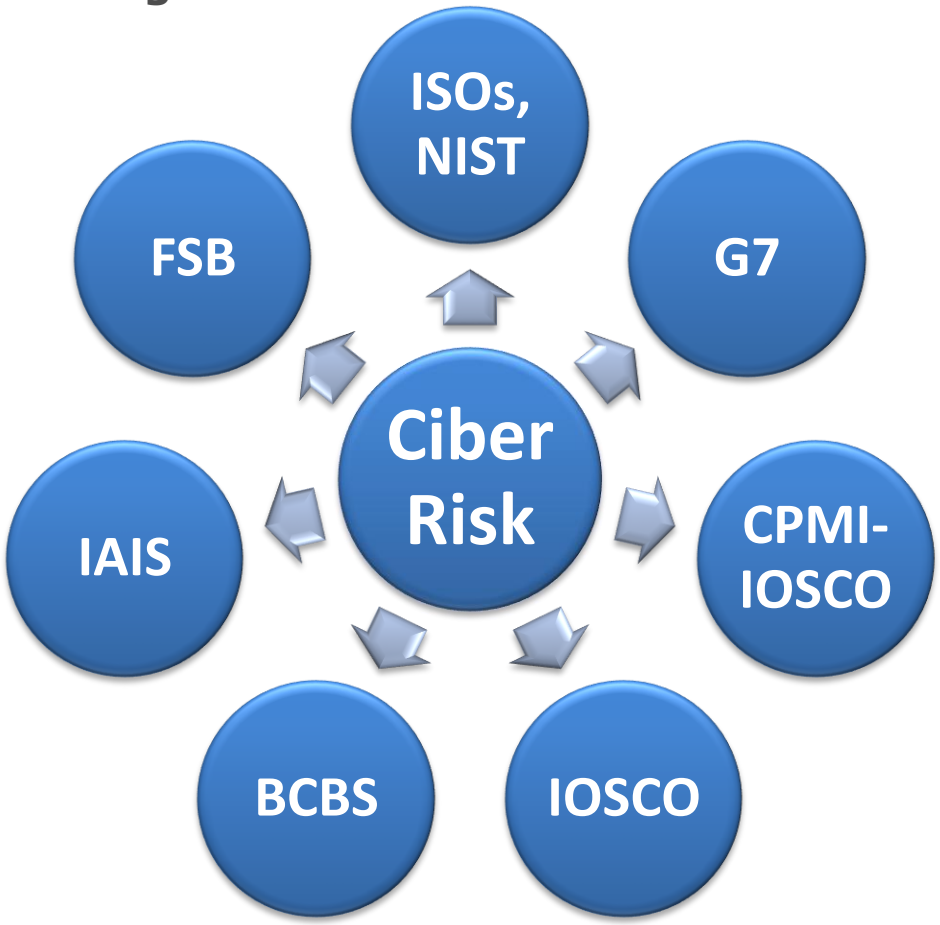
Chile's BancoEstado falls victim to ransomware attack

The hackers are believed to be criminal cybergang REvil.

Ruby Hinchliffe
September 9, 2020

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

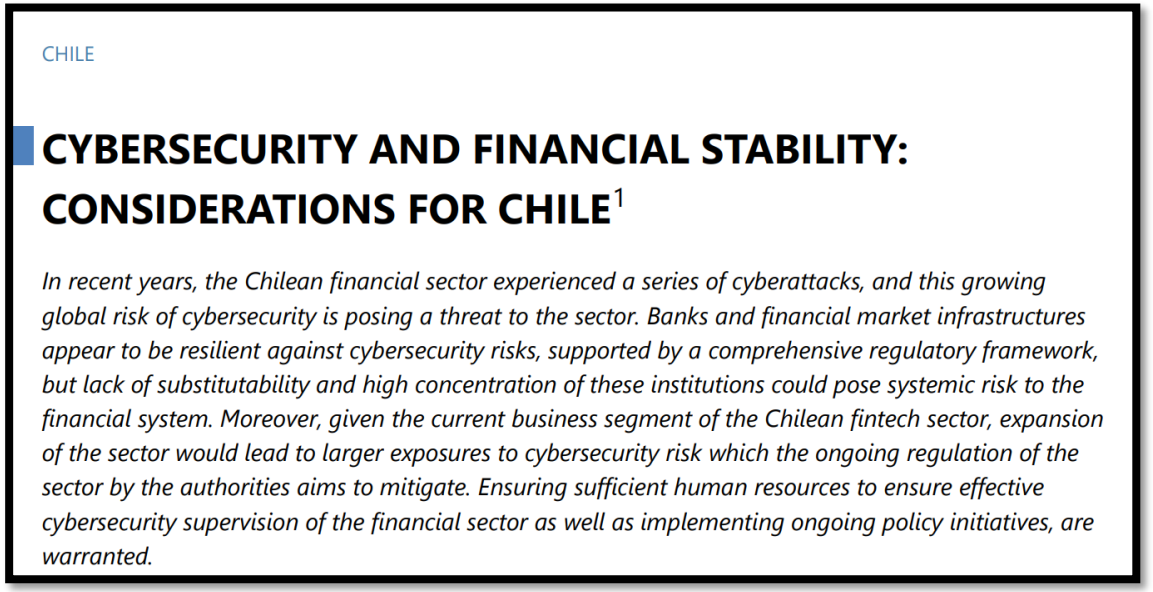


DORA
NIS 2
TIBER-EU

Lineamientos de supervisión y regulación
CBEST

El FMI (2024) realizó una evaluación sobre los avances de ciberseguridad y la importancia de abordar este riesgo para el resguardo del sistema financiero, emitiendo observaciones y recomendaciones…

- El FMI observa alta resiliencia ante ciberataques, pero alta concentración en grandes "puntos únicos de falla" (Redbanc, ComBanc, DCV o LBTR del BCCh).
- El marco regulatorio es sólido, pero con desafíos en el entrenamiento de los equipos, especialmente considerando las entradas en vigor de Ley Fintec y Ley Marco de Ciberseguridad.
- Como recomendación general: fortalecer capacidades internas, aumentar la coordinación e incluir pruebas de estrés cibernéticas.



CHILE

CYBERSECURITY AND FINANCIAL STABILITY: CONSIDERATIONS FOR CHILE[1]

In recent years, the Chilean financial sector experienced a series of cyberattacks, and this growing global risk of cybersecurity is posing a threat to the sector. Banks and financial market infrastructures appear to be resilient against cybersecurity risks, supported by a comprehensive regulatory framework, but lack of substitutability and high concentration of these institutions could pose systemic risk to the financial system. Moreover, given the current business segment of the Chilean fintech sector, expansion of the sector would lead to larger exposures to cybersecurity risk which the ongoing regulation of the sector by the authorities aims to mitigate. Ensuring sufficient human resources to ensure effective cybersecurity supervision of the financial sector as well as implementing ongoing policy initiatives, are warranted.

Con todo, la evaluación de ciberseguridad en Chile está en un nivel medio-alto en comparación a países comparables por ingreso y en la región

El Índice Nacional de Ciberseguridad (NCSI) mide aspectos de institucionalidad, respuesta, cooperación, capacidades y otras.

La reciente evaluación de Chile (2025) destacó avances considerables en:

- Institucionalidad
- Formación
- Infraestructura

NCSI :: Chile

La CMF también ha tomado medidas para enfrentar estas amenazas, pues la ciberseguridad se vincula con sus tres mandatos:

Nuestras acciones se desarrollan dentro de un marco legal en continuo fortalecimiento

Contexto local

- Política Nacional de Ciberseguridad
- Ley N° 19.628 sobre Protección de la Información
- Ley de Fraude (Ley N° 20.009)
- Ley N°21.459 de Cibercrimen

Leyes sectoriales

- Ley General de Cooperativas / Ley General de Bancos
- Ley de Seguros / Reglamento de los Auxiliares del Comercio de Seguros
- Ley de Mercados de Valores / Ley Única de Fondos / Leyes de Infraestructuras (DV, ECC)

Leyes recientes

- Ley Marco de Ciberseguridad (Ley N° 21.663)
- Modificaciones a la Ley de Protección de Datos Personales (Ley N° 21.719) y Ley de Fraudes (Ley N° 21.673)
- Ley Fintec (Ley N° 21.521)

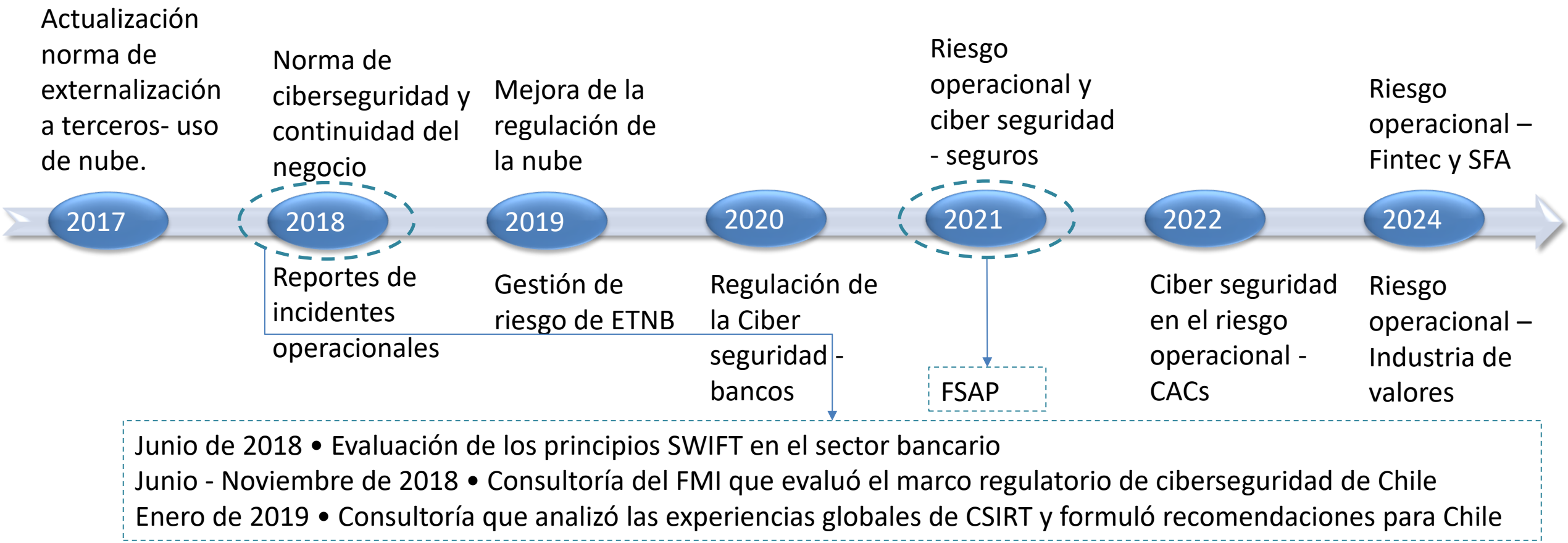
Fortalecimiento de la supervisión y regulación

Continuo Monitoreo a través de industrias

Poderes legales para acciones adicionales

Implementación de Basilea 3

Hace varios años se ha estado avanzando en nuestro perfeccionamiento regulatorio



Junio de 2018 • Evaluación de los principios SWIFT en el sector bancario
Junio - Noviembre de 2018 • Consultoría del FMI que evaluó el marco regulatorio de ciberseguridad de Chile
Enero de 2019 • Consultoría que analizó las experiencias globales de CSIRT y formuló recomendaciones para Chile

*La regla original fue emitida en 2000..

Nuestro enfoque prudencial (pero proporcional) en materia de regulación cibernética

Gobierno corporativo

- Rol del directorio
- Estructura organizacional
- Políticas y procedimientos
- Cultura y conciencia del riesgo
- Desarrollo de capacidades
- Gestión de alertas y amenazas

Gestión de la información

- Identificación de activos de información.
- Control de acceso y monitoreo
- Identificación y detección de amenazas
- Gestión de respaldos
- Evaluación de controles
- Procedimientos de gestión de incidentes
- Mejora continua y testeo

Gestión de la ciber seguridad

- Clasificación de los activos críticos
- Gestión del cambio
- Obsolescencia, configuración y parches
- Protección de la red
- Plan de recuperación y testeo
- Comunicación y planes de acción

Nuestra regulación fomenta el intercambio de información sobre incidentes cibernéticos en toda la industria financiera

COMISIÓN PARA EL MERCADO FINANCIERO

GRUPOS DE TRABAJO SECTORIALES CRECEN EN EL MUNDO:

Colaboración, estrategia esencial contra las ciberamenazas

En Chile, la Virtual Task Force coordina esfuerzos entre 27 instituciones financieras, lo que les ha permitido aplicar medidas proactivas y hacer frente a amenazas.

NOEMÍ MIRANDA G.

La veloz evolución del cibercrimen, tanto en cantidad como en grado de sofisticación, lo ha llevado a ser definido como una fuerza disruptiva que amenaza a la sociedad como un todo, indica el reciente reporte Global Cybersecurity Outlook 2025, del Foro Económico Mundial.

Y el sector financiero es uno de los principales blancos: si en 2022 se reportaron 1.829 ataques, la cifra en 2023 casi se triplicó, registrándose 3.348 incidentes, según Statista.

Frente a ello, se han puesto en marcha diversas medidas para mejorar la ciberseguridad, y una de las fundamentales tiene que ver con la colaboración sectorial. En Chile, adelantándose a las tendencias, desde 2017 existe la Virtual Task Force (VTF), una iniciativa de la Asociación de Bancos e Instituciones Financieras (ABIF) que coordina esfuerzos en ciberseguridad entre 27 empresas del rubro. "Su creación se inspiró en modelos de colaboración implementados en el Reino Unido, donde instituciones policiales lideraron estrategias conjuntas de seguridad cibernética con la industria financiera", explica Cristián Vega, gerente de Operaciones y Tecnología de la ABIF. Un principio clave que guía a la VTF, agrega, es que en temas de ciberseguridad no se compite; esto permitió que el grupo de trabajo y sus definiciones se implementaran sin una normativa que obligara a sus miembros.

EL MERCURIO

Un principio clave es que en ciberseguridad no se compite.

"Actualmente, la VTF se relaciona con organismos como el Instituto Nacional de Ciberseguridad de España (Incibe) y la Federación Brasileña de Bancos (Febraban), para fortalecer su capacidad de respuesta y aplicar medidas proactivas. Estas acciones han permitido a la industria enfrentar amenazas como *ransomware*, ataques de denegación de servicio y vulnerabilidades en proveedores críticos", señala Vega.

Los principios que promueve la VTF están en sintonía con la reciente Ley DORA que, en Europa, obliga al mundo financiero a incrementar su ciberseguridad; ambas buscan fortalecer la resiliencia operativa digital del sector, para que las empresas puedan resistir, responder y recuperarse de incidentes sin comprometer la estabilidad del sistema financiero. "Uno de los aspectos más relevantes que comparten es la gestión de riesgos en la cadena de suministro y proveedores críticos, un área en la que la banca chilena ve oportunidades de mejora y maduración para fortalecer la seguridad del ecosistema. La nueva Ley de Ciberseguridad en Chile también incorpora estos elementos, alineándose con las mejores prácticas internacionales", indica Vega.

Ahora bien, "la efectividad de este enfoque depende de factores como el presupuesto, la capacidad de ejecución y el nivel regulatorio de cada industria. Si bien compartir información es clave, la respuesta a un ataque debe adaptarse a la realidad de cada empresa, ya que estos eventos suelen explotar vulnerabilidades específicas de la organización en lugar de atacar a toda la industria", comenta Marcelo Díaz, socio del área de Cyber Risk de Deloitte Chile.

Unión público-privada

Erich Zschaeck, gerente sénior de Ciberseguridad de EY, comenta que la colaboración también se ha dado entre el mundo público y el sector privado: "En Chile, la Agencia Nacional de Ciberseguridad (ANCI) pretende ser un actor clave para impulsar este tipo de iniciativas. A nivel internacional, destacan la Cybersecurity and Infrastructure Security Agency (CISA) en Estados Unidos, que brinda recursos y colaboración público-privada para proteger infraestructuras críticas. En Europa, la EBA (European Banking Authority) desarrolla directrices y marcos regulatorios para la ciberseguridad en el sector bancario. Por otra parte, Mitre ATT&CK es una base de datos sin fines de lucro que documenta tácticas y técnicas de adversarios en ciberseguridad, facilitando la defensa proactiva y la mejora de estrategias de protección", detalla.

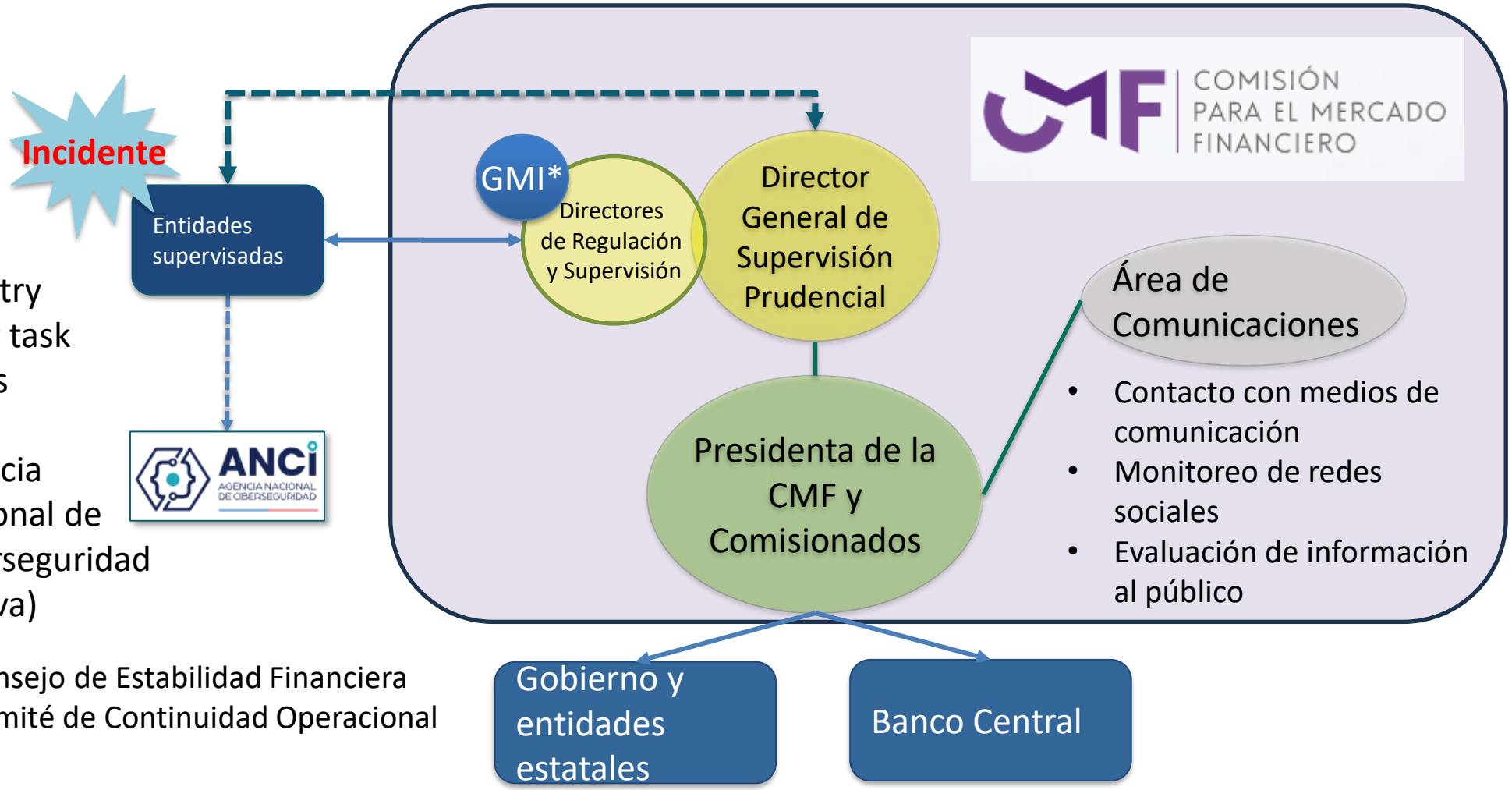
ANCI publica lista preliminar de Operadores de Importancia Vital y abre consulta pública

La Agencia Nacional de Ciberseguridad identificó 1.712 instituciones públicas y privadas de energía, salud, telecomunicaciones, servicios digitales, servicios financieros y del Estado como OIV en el marco de la Ley Marco de Ciberseguridad.

La Regulación de Cooperativas de Ahorro y Crédito se encuentra en un proceso de modernización relevante:

- La Circular N° 108 de CACs establece **lineamientos sobre ciberseguridad** → Cita al Capítulo 20-8 de la RAN de Bancos.
- Lo mismo realiza para la **externalización de servicios**, en relación al Capítulo 20-7 de la RAN; para **continuidad del negocio** (20-9) y para **transferencia de información y activos** (1-7).
- La **Ley de Resiliencia Financiera**, publicada el día 30.12.23, estableció un amplio rol de la CMF en términos de evaluación de gestión de riesgo, incluyendo el de ciberseguridad, dado que el fin de asegurar la continuidad operativa e integridad de los servicios críticos en esta industria dentro del sistema financiero.
- Para implementar lo anterior, ya se sometió a una consulta pública y se planea emitir este año la normativa correspondiente en una **Recopilación Actualizada de Normas para CACs.**

Nuestro enfoque de supervisión frente a incidentes de seguridad



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

Industry cyber task forces

Agencia Nacional de Ciberseguridad (nueva)

- Consejo de Estabilidad Financiera
- Comité de Continuidad Operacional

Actividades

1. Establecimiento y mantenimiento de contacto
2. Intercambio y análisis de información
3. Escalada de incidentes
4. Definición de acciones de supervisión
5. Monitoreo
6. Cierre

*GMI: Grupo de monitoreo de incidentes, compuesto por representantes de ambas Direcciones

Caso práctico

- En septiembre de 2020, un *ransomware* afectó miles de equipos de una entidad financiera de la plaza.

- El *malware* afectó aproximadamente 12.000 equipos (estaciones de trabajo y servidores) cifrando archivos con información en formato Office (plataforma Windows).

- Los principales servicios y plataformas afectados fueron: correo electrónico corporativo, sistemas de caja y ventanilla de sucursal, plataforma empresarial, sitios web corporativos, mercados de capitales y mesa de dinero.

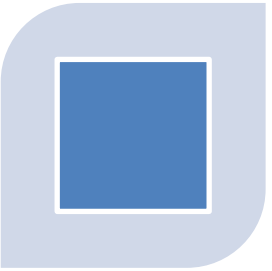
Evolución del incidente

Notificación y reporte

DIA 0: INFORME DE INCIDENTES OPERATIVOS Y MEDIDAS INICIALES (RIO, SUPERVISIÓN INSITU, COORDINACIÓN CON INDUSTRIA, CEF)

DIA 1: MÁS INFORMACIÓN SOBRE EL INCIDENTE, SERVICIOS AFECTADOS Y PLAN DE ACCIÓN PARA ELIMINAR EL MALWARE, COMUNICADO DE PRENSA

DIA 2: ESTADO DE AVANCE DE MEDIDAS, REUNIÓN CON PRESIDENTE CMF, DECLARACIÓN PÚBLICA



DIA 3: NUEVOS AVANCES DE MEDIDAS, COODINACIÓN DE RECUPERACIÓN

Estrategia Supervisora

El enfoque del CMF es siempre monitorear la evolución y resolución de los incidentes.
Nuestra estrategia de comunicación fue crucial y abarcó a todas las partes interesadas relevantes.

Con la Institución Financiera

- Supervisión se reunía diariamente
- Despliegue in-situ
- Contacto con filiales
- Solicitud de más información

Con autoridades y la industria

- Actualización diaria al Comité del Consejo de Estabilidad Financiera (Banco Central de Chile y otros)
- Coordinación con el Ministerio del Interior
- Coordinación con la industria y sus grupos de continuidad de negocio

Al público

- Comunicado
- Declaración pública
- Seguimiento de la información proporcionada a los clientes
- Reporte a la Comisión de Economía del Senado

Cooperación: a nivel nacional

Este caso práctico demuestra que la cooperación es clave para mantener un sistema financiero resiliente.
Entre 2025 y 2026, Chile dará la bienvenida a dos nuevas agencias destinadas a fortalecer la gestión nacional de la ciberseguridad y la protección de datos.

Agencia de Ciberseguridad

- Gestiona el CSIRT Nacional
- Debe coordinarse con la agencia sectorial correspondiente.

Agencia de Protección de Datos

- Inspirada en el RGPD, regula la protección y el tratamiento de datos.
- La agencia debería estar establecida para diciembre de 2026.

Cooperación: a nivel internacional

Asistencia y apoyo técnico	• 2018 – Evaluación cibernética del FMI • 2022 – Reunión con especialistas de la OICV sobre resiliencia operativa
Ejercicios de simulación	• 2022-23 – Ejercicio de simulación cibernética de la Alianza del Pacífico (apoyo del BID) • Además de la ciberseguridad, hemos participado en simulacros de crisis.
Fortalecimiento de capacidades	• Talleres sobre ciberseguridad y tecnología impartidos por la Alianza del Pacífico • Participación en diversos talleres impartidos por organizaciones internacionales.
Intercambio de experiencias	• Aprendizaje mutuo y comunicación continua. Modernización de los memorandos de entendimiento. • Participamos activamente en los colegios de supervisores.

Conclusiones y Desafíos Futuros

- 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 se encuentran entre nuestras múltiples prioridades
- Los requisitos actuales, nuevos y futuros (por ejemplo, un mayor capital basado en el riesgo) son (y serán) útiles.
- La experiencia empírica demuestra que la cooperación y la comunicación interinstitucionales son cruciales para una gestión eficaz de incidentes.
- En paralelo, existen otros desafíos apareciendo en el radar: evolución de criptoactivos, IA, computación cuántica y más…
- En este sentido, los reguladores deben ser proactivos para tomar medidas regulatorias y de supervisión oportunas.
- Esto, en el contexto de la implementación de la Ley de Resiliencia Financiera, pareciera ser una gran oportunidad para avanzar en el sector cooperativo con reglas más claras, proporcionales, que se enfoquen en el riesgo y en los propósitos de un sistema financiero más estable y resiliente.

100 años de regulación y supervisión bancaria

COMISIÓN PARA EL MERCADO FINANCIERO

Ciberseguridad: La experiencia de la CMF

Francisco Cabezón Ferraté
Director General de Regulación Prudencial
24 de Octubre de 2025