Ciberseguridad en el Sistema Financiero

Joaquín Cortez Huerta

19 de junio de 2018

COMISIÓN
PARA EL MERCADO
FINANCIERO

Perímetro de Supervisión

COMISIÓN PARA EL MERCADO FINANCIERO

Comisión Para el Mercado Financiero (CMF)

Intendencia de Valores (2.259)

- Infraestructura de Mercado
- Intermediarios
- Emisores
- Fondos y Administradoras
- Clasificadoras y Auditores

Intendencia de Seguros (5.031)

- Vida
- Generales
- Corredores y Liquidadoras

Perímetro de Supervisión
Enfoque Supervisión Basado en Riesgo (SBR)

COMISIÓN PARA EL MERCADO FINANCIERO

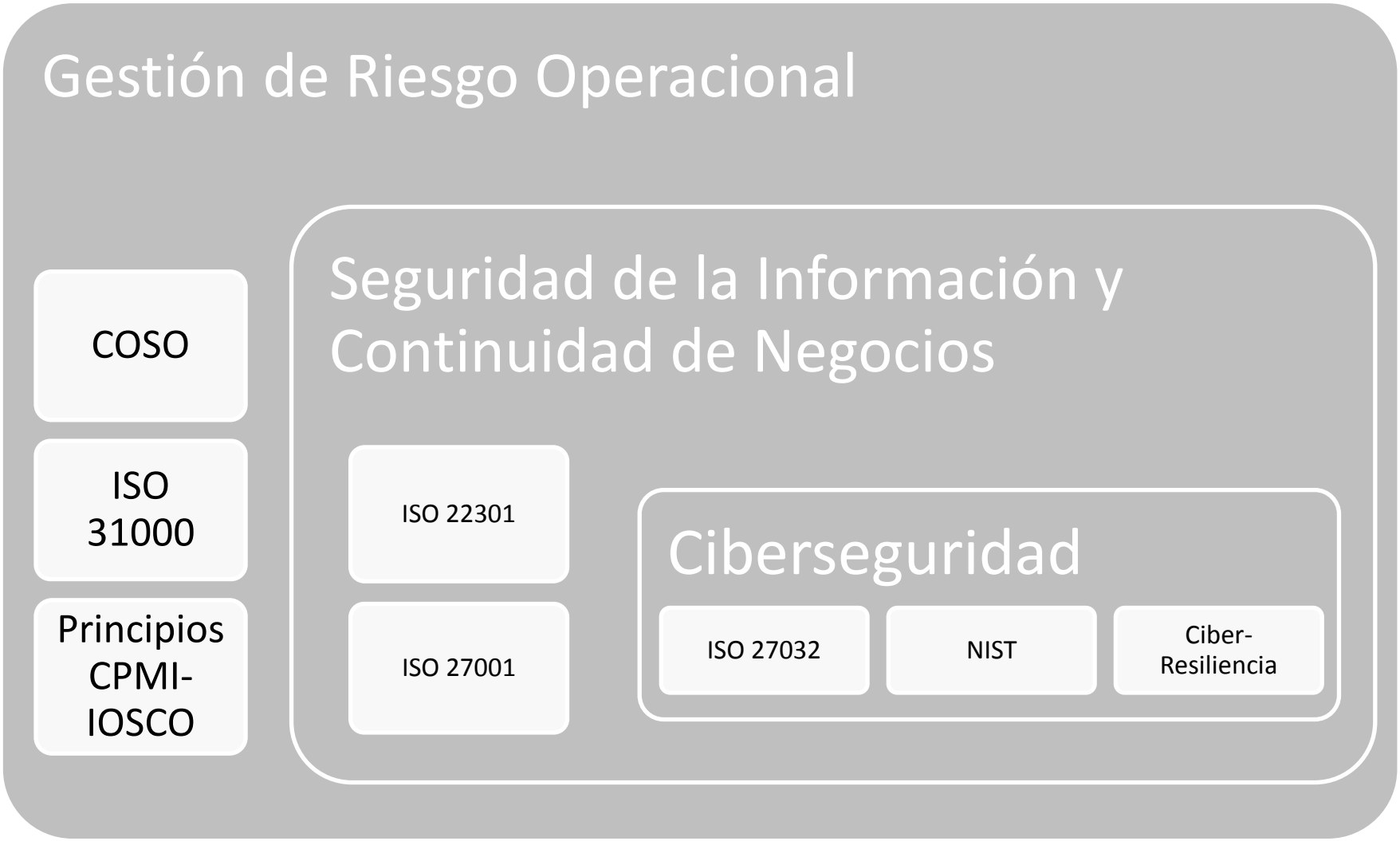
- Desde hace algunos años, la CMF aplica a sus entidades fiscalizadas el enfoque de **Supervisión Basada en Riesgos (SBR)**, cuyo propósito es que las entidades cuenten con debidos procesos de gestión de riesgos.

- En este sentido, la CMF ha emitido diversas normativas mediante las cuales exige a las entidades implementar procesos de gestión para sus riesgos relevantes.
  - Entre éstos se encuentran los riesgos operacionales, que incluyen los riesgos de seguridad de la información y de continuidad de negocios (que incluyen la Ciberseguridad).

- La labor de supervisión de la CMF se orienta a verificar el debido cumplimiento de estas normativas, exigiendo las mejoras necesarias en caso de observarse algún proceso/riesgo que no está debidamente gestionado.

Perímetro de Supervisión
Contexto de Estándares Internacionales

COMISIÓN PARA EL MERCADO FINANCIERO



Perímetro de Supervisión
Ciberseguridad

COMISIÓN PARA EL MERCADO FINANCIERO

- En materia de riesgo operacional (incluido Ciberseguridad), un ámbito de relevancia mayor para el sistema financiero corresponde a las **Entidades de Infraestructura de Mercado (EIM)**.
  - EIM: Entidades de depósito y custodia; sociedades administradoras de sistemas de compensación y liquidación; bolsas de valores.
  - Las EIM proveen la infraestructura para la realización, custodia, compensación y liquidación de las transacciones de valores, por tanto, la continuidad operacional de sus servicios y sistemas resulta crítica.
  - Uso intensivo de las tecnologías de la información.
  - Interconexión y carácter sistémico.

- Asimismo, la gestión de riesgo operacional es de alta relevancia en el caso de los **Intermediarios de Valores**, **Administradoras de Fondos** y **Compañías de Seguros**.

(1) Entidades de Infraestructura de Mercado

COMISIÓN PARA EL MERCADO FINANCIERO

DCV

- Empresa de depósito y custodia (Ley N°18.876)
- Valores de oferta pública inscritos en la CMF y SBIF, emitidos por BC y Estado
- Otros autorizados por CMF por NCG
- Valores custodiados MMUS$ 395.174

CCLV

- Sociedades Adm. de Sistemas de Compensación y Liquidación (Ley N° 20.345)
- Operaciones bursátiles de IIF, RF, RV y Derivados
- Saldos liquidados MMUS$ 390.342 (2017)

COMDER

- Sociedades Adm. de Sistemas de Compensación y Liquidación (Ley N° 20.345)
- Derivados OTC de inflación, tasas y monedas
- Saldos liquidados MMUS$ 6.182 (2017)

Bolsas de Valores

- Bolsa de Valores (Ley N° 18.045)
- **BCS**
- Transacciones 2017 en valores MMU$ 480.788 (98% ops. bursátiles)
- **BEC**
- Transacciones 2017 en valores MMU$ 11.464 (2% ops. bursátiles)
- **BV**
- Transacciones 2017 en valores MMU$ 10.
- **BP**
- Ley N° 19.220
- Operaciones 2017 por MMU$ 1.950.

(1) Entidades de Infraestructura de Mercado

COMISIÓN PARA EL MERCADO FINANCIERO

- La CMF ha venido trabajando en el fortalecimiento de la supervisión de las EIM. Un último hito correspondió a la creación de una División que se hizo cargo de todas estas entidades, para efectos de aplicar procesos comunes de SBR.

- La supervisión del riesgo operacional en las EIM, es realizada sobre la base de un marco normativo de gestión de riesgos.
  - *Circular N° 1939: Gestión de riesgo operacional.*
  - *Circular N° 2020: Comunicación, gestión y resolución de incidentes operacionales críticos.*

  Ambas para entidades de depósito y custodia de valores y sociedades administradoras de sistemas de compensación y liquidación de instrumentos financieros.

- Si bien estas normas no exigen la implementación de estándares internacionales sobre riesgo operacional, por parte de las EIM, el enfoque de fiscalización las considera como guía al momento de evaluar la gestión.

Anexo

(1) Entidades de infraestructura de Mercado

COMISIÓN PARA EL MERCADO FINANCIERO

- Como resultado de las actividades de fiscalización, se aprecia un alto estándar de gestión de los riesgos operacionales en las principales EIM.
  - Existencia de procesos basados en estándares internacionales de **continuidad de negocios** y **seguridad de la información**. Procesos certificados por entidades internacionales.
  - Implementación de buenas prácticas (hackeo ético, autoevaluación).
  - Adecuada infraestructura tecnológica.

Anexo

- En este mismo sentido, en el año 2015 el Banco Mundial y el FMI realizaron una evaluación sobre el cumplimiento local de los principios internacionales aplicables a las infraestructuras financieras. Su resultado dio cuenta de un alto nivel de cumplimiento, por parte de las entidades y autoridades.
  - No obstante, se identificó algunas brechas a ser abordadas, entre ellas, fortalecer el marco legal y regulatorio en determinados aspectos.
  - En línea con lo anterior, la CMF se encuentra evaluando la emisión en el corto plazo de una normativa específica en esta materia adoptando principios de infraestructura de mercado desarrollados por IOSCO.

(2) Intermediarios de Valores y Administradoras de Fondos

COMISIÓN PARA EL MERCADO FINANCIERO

(Corredores de Bolsa y Agentes de Valores: 45)

(Administradoras Generales de Fondos: 49)

- La CMF emitió en 2008 y 2011, respectivamente, el marco normativo de supervisión:
  - *Circular N° 1869, gestión de riesgos y control interno en administradoras de fondos.*
  - *Circular N° 2054, control interno y gestión de riesgos para intermediarios.*

- En este sentido, el enfoque de supervisión, en el ámbito de riesgo operacional, se orienta a evaluar la existencia y razonabilidad del marco de políticas y procedimientos sobre la materia, como también las actividades asociadas a la definición y aplicación de planes de continuidad operacional.

- En el ámbito de seguridad de la información y ciberseguridad, nuestro alcance ha sido acotado.

(2) Intermediarios de Valores y Administradoras de Fondos

COMISIÓN PARA EL MERCADO FINANCIERO

Espacios de Mejora y Desafíos

- Revisar el marco normativo con el objeto de evaluar la incorporación de instrucciones sobre estos riesgos específicos.

- Fortalecer nuestro esquema de supervisión en este ámbito:
  - Seguir profundizando nuestras evaluaciones en el ámbito de riesgo operacional.
  - Incorporar actividades orientadas a evaluar la suficiencia de las definiciones y aplicaciones en el ámbito de los riesgos de seguridad de información y ciberseguridad.

- Reforzar nuestro equipo de profesionales, con miras a hacernos cargo de estos nuevos desafíos.

(3) Compañías de Seguros

(Compañías de seguros de vida: 32)
(Compañías de seguros generales: 37)

- El marco normativo en este ámbito para las compañías de seguros se encuentra comprendido en las normativas de carácter general 309 y 325. En ellas el riesgo operacional, definido como el riesgo de pérdidas financieras que resulta de fallos en los procesos, personas o sistemas, ya sea ante eventos internos o externos, incluye el riesgo de tecnologías de información (TI).

- Para evaluar este aspecto, la CMF supervisa en terreno y en gabinete la existencia de políticas, procedimientos y planes de prueba que aplican para gestionar los riesgos asociados a:
  - Sistemas informáticos.
  - Outsourcing.
  - Continuidad del negocio.
  - Recursos humanos inadecuados.
  - Fraude interno y externo.
  - En general los riesgos relacionados con los procesos operacionales.

- La CMF supervisa que las aseguradoras cuenten con un Plan de Continuidad del Negocio (PCN), debidamente actualizado, el que debe abordar aspectos de ciberseguridad.

(3) Compañías de seguros

Espacios de Mejora y Desafíos

- En el corto plazo:
  - Reforzar las acciones de supervisión respecto de los Planes de Continuidad Operacional de las compañías, poniendo énfasis en ciberseguridad.
  - Generar un trabajo público/ privado que aborde los distintos aspectos de ciberseguridad en compañías de seguro.

- En el mediano y largo plazo:
  - Aprobación del proyecto de Ley de Supervisión Basada en Riesgo que establezca exigencias de capital en función de la evaluación de riesgos de las compañías.
  - Actualización normativa y metodología de evaluación de gestión de riesgo operacional, incluyendo lo relacionado a ciberseguridad.
  - Fortalecer la supervisión en TI para lo cual es necesario contar con los recursos humanos y tecnológicos adecuados.

Conclusiones

COMISIÓN PARA EL MERCADO FINANCIERO

- En general la supervisión realizada por la CMF incorpora dentro de sus protocolos la supervisión del riesgo operacional, donde se encuentra la gestión del riesgo de ciberseguridad.

- En el caso de las Entidades de Infraestructura de Mercado, los antecedentes dan cuenta de un alto estándar de gestión del riesgo operacional en las principales EIM.
  - Este ámbito debiera ser fortalecido mediante normas específicas sobre la materia, entre ellas, sobre la aplicación de los PFMI.

- En el caso de los Intermediarios de Valores, Administradoras de Fondos y Compañías de Seguro, si bien la CMF ha impartido instrucciones sobre la gestión de riesgos y evaluado la gestión de riesgos operacionales, nuestro desafío es fortalecer el marco regulatorio específico sobre ciberseguridad, así como profundizar la fiscalización en esta materia.

- Para ello, la CMF se encuentra evaluando la necesidad de requerir una consultoría externa orientada a identificar y abordar las brechas en esta materia, en cuanto a:
  - Marco regulatorio.
  - Procedimientos de fiscalización.
  - Dotación de recursos especializados.

Anexo - Estándares Internacionales

COMISIÓN PARA EL MERCADO FINANCIERO

- ISO 31000: Gestión de Riesgos.
- ISO 22301: Gestión de la Continuidad de Negocios.
- ISO 27001: Gestión de la Seguridad de la Información.
- ISO 27032: Gestión de la Ciberseguridad.
- Cybersecurity Framework (NIST: National Institute of Standards and Technology).
- CPMI-IOSCO: Principios aplicables a Infraestructuras de Mercado.
- CPMI-IOSCO: Guía sobre Ciber-Resiliencia en Infraestructuras de Mercado.
- COSO: Committee of Sponsoring Organizations of the Treadway.

Volver

Anexo – Principales Entidades Infraestructura de Mercado

COMISIÓN PARA EL MERCADO FINANCIERO

	DCV	CCLV	COMDER	BCS
Continuidad de Negocios				
Procesos basados en ISO 22301	SI	SI	SI	SI
Certificación ISO 22301	SI	SI	SI	SI
Posee identificación de procesos críticos	SI	SI	SI	SI
Posee planes de continuidad de negocio	SI	SI	SI	SI
Realiza pruebas/ejercicos de continuidad	SI	SI	SI	SI
Seguridad de Información				
Procesos basados en ISO 27001	SI	SI	SI	SI
Certificación ISO 27001		SI	SI	SI
Posee gestión de incidentes	SI	SI	SI	SI
Posee gestión de crisis	SI	SI	SI	SI
Ciberseguridad				
Procesos basados en ISO 27032			SI	
Ethical Hacking	SI	SI	SI	SI
Autoevaluación (CPMI-IOSCO/NIST)	SI	SI	SI	SI
Datacenter				
Datacenter principal Tier III	SI	SI	SI	SI
Datacenter de respaldo	SI	SI	SI	SI
Datacenter de respaldo Tier III		SI	SI	SI
Tercer Datacenter	SI		SI	

Volver