COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Regulación y ciberseguridad en el sistema financiero

Bernardita Piedrabuena K.
Vice Presidenta
Comisión para el Mercado Financiero

Sexta Charla Informativa, ACAFI, 7 de agosto de 2024

Motivación

- En cumplimiento de su mandato legal, a la Comisión para el Mercado Financiero le corresponde velar por el correcto funcionamiento, desarrollo y estabilidad del mercado financiero, para lo cual cuenta con sus atribuciones de regulación y fiscalización.

- Para ello, utiliza una metodología de supervisión basada en riesgos, la cual implica, entre otras cosas, una focalización en las actividades de las entidades supervisadas que pudieran tener un mayor impacto en caso de materializarse algún riesgo inherente a su giro.

- En el caso de la industria bancaria y seguros, se contaba con normas comprehensivas y actualizadas. Las normas recientemente publicadas vienen a completar, complementar y actualizar la normativa aplicable a intermediarios del sistema financiero:
  - Es importante aplicar estándares consistentes para todos los actores del mercado, ya que si un actor falla, esto puede tener efectos sobre todo el resto de los actores.

- El marco normativo para la gestión de riesgo operacional abarca la supervisión de aspectos de riesgo operacional tales como seguridad de la información, continuidad operacional y externalización de servicios.

Regulación sobre gestión de riesgo y ciberseguridad

2016

RAN 20-9
Continuidad de negocio para bancos,

2018

RAN 1-13
Clasificacion de gestión y solvencia de bancos (ciberseguridad).

RAN 20-8
Información de incidentes para bancos.

2019

RAN 20-7
Externalización de servicios para bancos.

2020

RAN 20-10
Gestión seguridad de la información y ciberseguridad para bancos.

2021

NCG 454
Riesgo operacional y ciberseguridad para compañías de seguros.

2022

Circular 2.304
Riesgo operacional para cooperativas de ahorro y crédito.

2024

NCG 507, 508, 509
Normas de gestión integral de riesgos para intermediarios y AGF.

NCG 510
Normas de gestión de riesgo operacional para intermediarios y AGF (ciberseguridad).

Componentes claves en la gestión de riesgos cibernéticos

Gobierno corporativo	Planeación y preparación	Análisis	Mitigación	Restauración y recuperación	Coordinación y comunicación	Mejoramiento
Directorio	Políticas	Taxonomía	Contención	Priorización	Escalamiento	Iniciativas de la industria
Definición de roles y responsabilidades	Planes y libro de prácticas	Logs	Plan de continuidad operacional	Restauración de datos	Reporte	Análisis ex post, lecciones aprendidas
Coordinador de incidentes	Estrategia de comunicaciones: stakeholders, canales	Fuentes de información confiable	Aislación del incidente	"Golden source" data	Actualización situación	Ejercicios y pruebas, coordinación
Cultura	Escenario de tensión		Erradicación|	Hitos claves	Manejo de medios	Información externa
Presupuesto	SOC			Monitoreo	Coordinación con otros actores y autoridades	
Medición	Terceras partes y cadena de suministros					

Fuente: FSB, *Effective Practices for Cyber Incident Response and Recovery, Final Report*, octubre 2020.

Gobierno corporativo y gestión de riesgos

Elementos de proporcionalidad

Entidad	Comités de Directorio (u órgano equivalente)	Procedimientos de Gestión de Riesgos	Gestión de Riesgos y Auditoría Interna
Intermediarios de Valores y corredores de Bolsa de Productos.	**Comité de Riesgos obligatorio.** **Comités de Riesgos y de Auditoría** deberán estar integrados al menos por un miembro del directorio u órgano equivalente.	Adecuados para el volumen y complejidad de actividades de la entidad.	**Función de Gestión de Riesgos - Unidad de Auditoría Interna.** En función del volumen y complejidad de actividades de la entidad: • La Función de Gestión de Riesgos puede delegar parte de sus actividades en el encargado de cumplimiento, gerentes de área o en otra unidad corporativa de su holding (previo manejo de conflictos de interés). Si el volumen y complejidad de actividades es significativo, deberá crearse una Unidad de Gestión de Riesgos. • La Unidad de Auditoría Interna puede delegar parte de sus actividades en la unidad corporativa de su holding o en un tercero.
Administradoras Generales de Fondos.	**Comité de Riesgos obligatorio.** **Comités de Riesgos, Liquidez, PLAFT o Auditoría** deberán estar integrados al menos por un miembro del directorio.	Adecuados para el volumen y complejidad de actividades de la entidad.	**Unidad de Gestión de Riesgos – Unidad de Auditoría Interna.** En función del volumen y complejidad de actividades de la entidad: • La Unidad de Gestión de Riesgos puede delegar parte de sus actividades en el encargado de cumplimiento, gerentes de área o en otra unidad corporativa de su holding (previo manejo de conflictos de interés). • La Unidad de Auditoría Interna puede delegar parte de sus actividades en la unidad corporativa de su holding o en un tercero.
Bolsas de Valores y Bolsas de Productos.	**Comité de Riesgos obligatorio.** **Comités de Riesgos y de Auditoría** deberán estar integrados al menos por un miembro del directorio.	Adecuados para el volumen y complejidad de actividades de la entidad.	**Unidad de Gestión de Riesgos – Unidad de Auditoría Interna** En función del volumen y complejidad de actividades de la entidad, dichas unidades pueden delegar parte de sus actividades en la unidad corporativa de su holding (previo manejo de conflictos de interés).
Sistemas de Compensación y Liquidación - Depósito y Custodia.	**Comité de Riesgos obligatorio.** **Comités de Riesgos y de Auditoría** deberán estar integrados al menos por un miembro del directorio.	Adecuados para el volumen y complejidad de actividades de la entidad.	**Unidad de Gestión de Riesgos – Unidad de Auditoría Interna.** En función del volumen y complejidad de actividades de la entidad, dichas unidades pueden delegar parte de sus actividades en la unidad corporativa de su holding.

Gestión de riesgo operacional

Sistema de Gestión del Riesgo Operacional (SGRO)

- Políticas, procedimientos y controles que permitan la resiliencia operativa de la entidad, consistentes con el apetito al riesgo definido por el directorio u órgano equivalente.
- Líneas claras de responsabilidad sobre la gestión del riesgo operacional.
- Indicadores de medición del riesgo operacional que permitan evaluar y monitorear periódicamente el grado de exposición a los distintos riesgos, permitiendo establecer niveles de alerta y evaluar la eficacia de los controles adoptados.
- Políticas de capacitación del todo el personal en gestión de riesgo operacional.
- Procedimientos de mejoramiento continuo de la gestión de riesgo operacional (herramientas, procedimientos y controles), incluyendo el análisis de incidentes y pérdidas operacionales.

Gestión de riesgo operacional

Seguridad de la información y ciberseguridad

- Identificación
- Protección y detección
- Respuesta y recuperación

Continuidad de negocio

Externalización de servicios

Reporte de incidentes operacionales

Seguridad de la información y ciberseguridad

Identificación:

- Definir los activos de información críticos.
- Clasificar la información, considerando dimensiones de disponibilidad, confidencialidad e integridad.
- Llevar un inventario actualizado de activos de información.

Seguridad de la información y ciberseguridad

Protección y detección:

- Controles de acceso a instalaciones físicas.
- Herramientas de registro, control y monitoreo de las actividades realizadas por los usuarios.
- Procedimientos de acceso del personal y los clientes a los sistemas (otorgamiento, modificación, revocación).
- Herramientas y controles para la detección y monitoreo de ataques cibernéticos y actividades anómalas (ej. firewalls de aplicaciones web, sistemas de prevención de intrusos, sistemas anti-denegación de servicios, filtrado de correo electrónico, antivirus, etc.).
- Gestión de configuración de activos de información y actualización de seguridad de software
- Respaldo, transferencia, restauración y eliminación de información, tomando en consideración técnicas de encriptación y segmentación de redes.
- Procedimientos de almacenamiento, transferencia y respaldo de información en la nube.

Seguridad de la información y ciberseguridad

Respuesta y recuperación:

- Procedimientos de respuesta y recuperación ante incidentes que consideren la recuperación oportuna de las funciones críticas, los procesos de respaldo y soporte, los activos de información y las interdependencias con terceros.
- Procedimientos de comunicaciones para mantener informado en forma oportuna al directorio u órgano equivalente, a otras partes interesadas y a la CMF de las medidas adoptadas para resolver incidentes, incluyendo el cumplimiento de las normas de protección de datos personales y derechos del consumidor.
- Proceso de gestión de cambio con la implementación de pruebas integrales para asegurar que no hubiere un impacto adverso previo al paso de producción de un servicio o activo de información.
- Proceso de gestión de obsolescencia tecnológica del hardware y software.

Continuidad del negocio

- Análisis de Impacto del Negocio (BIA) que considere los tiempos máximos tolerables de recuperación, los tiempos objetivo de recuperación, los puntos objetivo de recuperación y los niveles mínimos aceptables de operación.
- Análisis de Impacto de Riesgo (RIA) que permita identificar los riesgos de posibles eventos de continuidad y las medidas preventivas para cumplir los objetivos del BIA.
- Plan de Continuidad del Negocio y Recuperación ante Desastres:
  - Realización de pruebas anuales, diseñadas en proporción al volumen y complejidad de las operaciones de la entidad.
  - Las pruebas deberán estar basadas en escenarios no sólo asimilables a eventos reales sino a eventos severos pero plausibles.
- Sitio secundario para reanudar las operaciones en caso de un evento de continuidad.

Externalización de servicios

- Identificar los servicios relevantes para el cumplimiento normativo, la seguridad de la información o la continuidad del negocio (servicios críticos).
- Identificar servicios que requieren aprobación del directorio u órgano equivalente para ser externalizados.
- Mantener un registro de servicios externalizados que describa en detalle el servicio, su fecha de inicio y término, el proveedor que lo prestó y las obligaciones contraídas por éste.
- Definir los elementos mínimos del contrato de prestación de servicios externalizados (eg. as obligaciones contraídas por el proveedor y las estrategias de término de la prestación).
- Procedimientos para la selección de proveedores, incluyendo un *due diligence*.
- Procedimientos para el monitoreo de proveedores, incluyendo la realización de auditoría de servicios por parte del proveedor o bien certificaciones o revisiones independientes.
- En el caso de subcontratación en cadena, el proveedor es responsable en última instancia de la calidad de la prestación del servicio contratado.

Reporte de incidentes operacionales

Registro y comunicación de incidentes

- Incidentes operacionales críticos.
- Plazo máximo de 3 horas para intermediarios y AGF.
- Directorio u órgano equivalente define encargado de reporte de incidentes.
- En caso de que lo requiera la CMF, la entidad elaborará un informe de las causas del incidente y las medidas adoptadas para su resolución.

Registro y comunicación de pérdidas

- Pérdida financiera resultante de la materialización de riesgo operacional
- Umbral de 150 UF.
- Criterios para elaborar el registro de pérdidas.

Criterios para el registro de pérdidas

- Contar con procesos documentados (la CMF podrá requerir su validación por auditores externos).
- Incluir totalidad de actividades y exposiciones.
- Cálculo de pérdidas brutas y pérdidas netas.
- Detalle de información descriptiva sobre las causas del evento de pérdida en proporción al importe bruto de la pérdida.

Ley de ciberseguridad y PdL de datos personales

Ley de ciberserseguridad:

- Banca, servicios financieros y medios de pago como servicios esenciales: deber de reportar al CSIRT nacional máximo en 3 horas y respuesta del CSIRT en coordinación con el Consejo de Estabilidad Financiera (CEF).
- Coordinación regulatoria: Deferencia para el regulador sectorial (CMF), previa emisión de norma conjunta que determines criterios para la evaluación de la equivalencia.
- Supervisión sectorial: la autoridad sectorial será competente para fiscalizar, conocer y sancionar las infracciones, así como ejecutar las sanciones según lo establece la normativa sobre ciberseguridad que hubiere dictado.

PdL de datos personales:

- Deber de reportar las vulneraciones a las medidas de seguridad a la Agencia de Protección de Datos personales y a los titulares en caso de datos datos personales sensibles, datos relativos a niños y niñas menores de catorce años o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial.

Palabras finales

- La ciberseguridad es tarea de todos: de las personas, de las empresas, del regulador, del país.
- La regulación se ha basado en principios generales de gestión de riesgos, definidos por organismos internacionales, y los hemos adaptado a la realidad nacional.

Desafíos continuos:

- ❖ Para la CMF: adoptar formas eficientes de supervisión; construir capacidad de respuestas frente a eventos de sus fiscalizados y propios; coordinación con la Agencia de Ciberseguridad y el CSIRT Nacional; educar a los usuarios de los servicios financieros.

- ❖ Para los fiscalizados: capacitar/concientizar al interior de las empresas; establecer cooperación interempresas en un ámbito de no competencia; educar a los clientes en las tecnologías y productos financieros.

COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Regulación y ciberseguridad en el sistema financiero

Bernardita Piedrabuena K.
Vice Presidenta
Comisión para el Mercado Financiero

Sexta Charla Informativa, ACAFI, 7 de agosto de 2024