Presentación Situación Incidente Operacional

Comisión de Economía del Senado

Mario Farren Risopatrón
Superintendente de Bancos e Instituciones Financieras

Junio 2018

Mandato institucional de la SBIF

- Supervisar y regular a los bancos y a otras instituciones financieras con el objetivo de mantener la estabilidad y solvencia del sistema financiero, en resguardo de los depositantes y el interés público.

- Preservar la **confianza de los depositantes** en el sistema bancario nos obliga a actuar en forma independiente y oportuna.

- El mandato de la SBIF se enmarca en la Ley General de Bancos (LGB) y en toda la normativa asociada a ella.

El sistema bancario se basa en la confianza

Balance del Sistema Bancario

(miles de millones USD)

Activos y pasivos consolidados del sistema bancario Abril de 2018

Nuestra supervisión

El marco de la SBIF incluye:

- **Marco regulatorio prudencial (leyes y normas) orientado a limitar las actividades y los diversos riesgos de las entidades financieras.** (Ejemplo típico de regulación prudencial es el requerimiento de adecuación de capital mínima. Otra normativa es aquella referida a los márgenes de crédito a relacionados y no relacionados del art. 84 de la ley). Normas Específicas en Riesgo Operacional
- **Enfoque de supervisión basado en riesgos (fiscalización),** orientado a verificar que las entidades financieras cumplan con el marco regulatorio prudencial y adhieran a sanas prácticas de gestión de los riesgos.

Nuestra supervisión

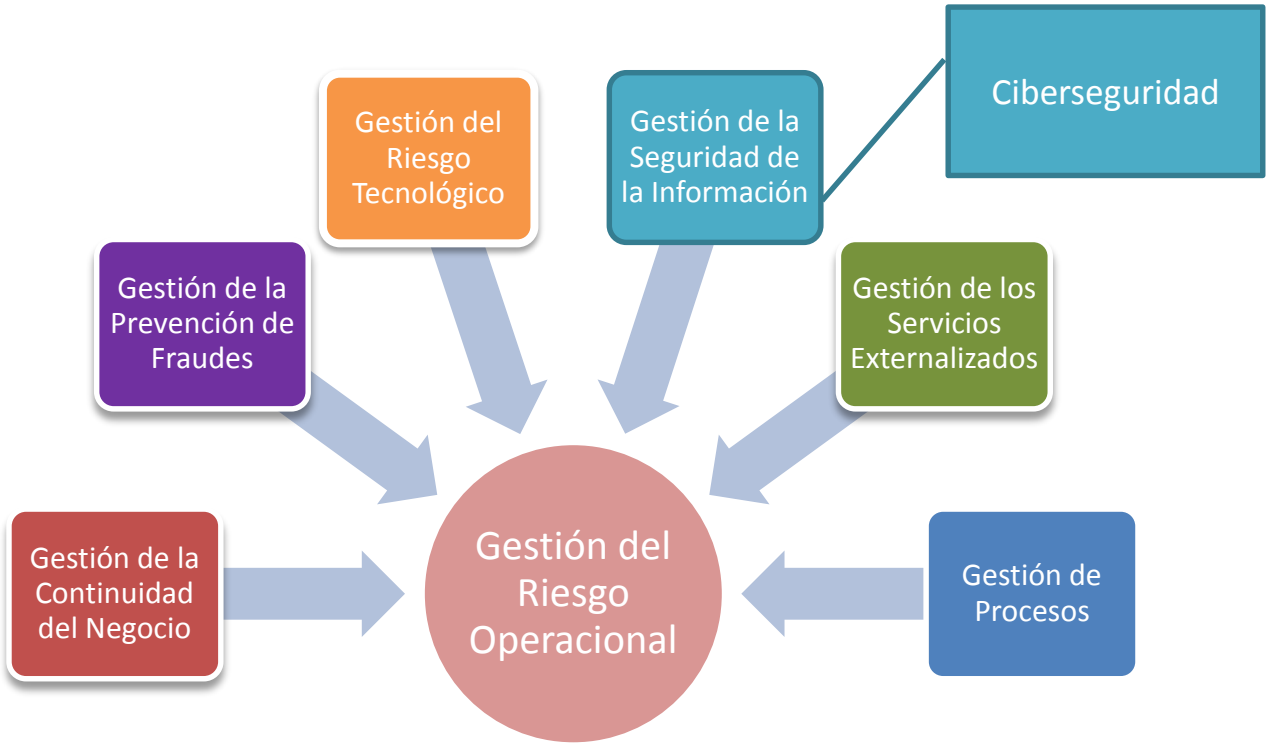
Supervisión basada en riesgos:

- El objeto de la supervisión es el banco como entidad.
- La supervisión basada en riesgos consiste en verificar la idoneidad de la gestión de los riesgos a que están expuestos los bancos.
- Para ello se revisan principalmente los riesgos de crédito, liquidez, mercado, **operacionales** y otros, así como los procesos que tiene el banco para su mitigación.

Supervisión del Riesgo Operacional

Superintendencia de Bancos e Instituciones Financieras Chile

SUPERVISIÓN DE LA GESTIÓN DEL RIESGO OPERACIONAL



Supervisión del Riesgo Operacional

Conceptualmente:

- **Gestión de riesgo tecnológico:** proceso de gestión que identifica posibles materializaciones de amenazas que explotan vulnerabilidades de los activos tecnológicos que soportan los procesos de negocio de la organización.
- **Gestión de seguridad de la información:** proceso mediante el cual una organización protege y asegura sus sistemas, medios de comunicación e instalaciones, de aquellos riesgos que pudieran atentar contra la integridad, confidencialidad y disponibilidad de la información vital de sus operaciones.
- **Ciberseguridad:** Comprende al conjunto de acciones para la protección de la información presente en el ciberespacio, así como de la infraestructura que la soporta.
- **Gestión de servicios externalizados**: proceso por el cual la entidad gestiona los riesgos asociados a la tercerizaciones de sus servicios.

Supervisión del Riesgo Operacional

- **Gestión de procesos:** Procesos mediante el cual la organización identifica, evalúa, controla, mitiga y monitorea los riesgos operacionales asociados a sus procesos estratégicos, de negocio y de apoyo.

- **Gestión de continuidad del negocio**: proceso de gestión que identifica las amenazas potenciales para la organización y los impactos que podrían tener una interrupción en la operación y que proporciona un marco a la organización para contar con la capacidad de recuperación.

- **Gestión de prevención de fraudes:** proceso que permite prevenir, detectar y dar respuesta a los riesgos de fraude, adoptando los controles necesarios y las acciones adecuadas y oportunas para la mitigación de éstos.

Supervisión del Riesgo Operacional

Como se aborda:

- **Gobierno sobre la Materia.** Esto incluye el rol del Directorio; la función de riesgos; los Comités. También aspectos organizacionales: estructura, roles y responsabilidades, segregación funcional.

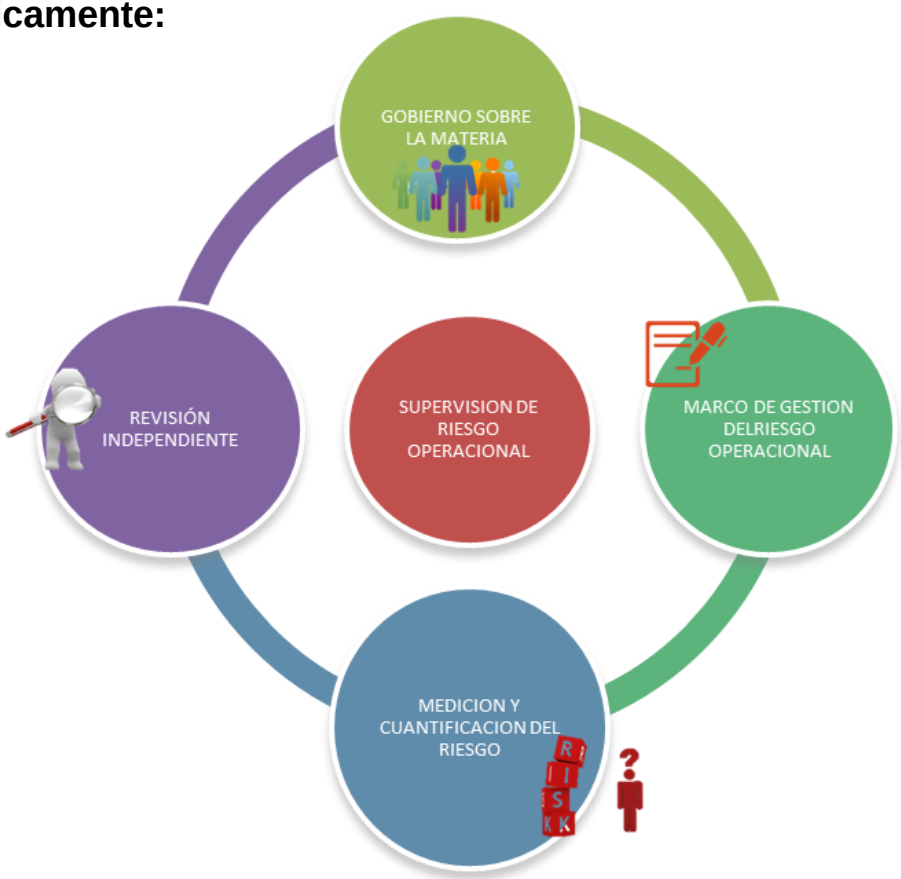
- **Marco de Gestión.** Incluye las políticas y procedimientos; atribuciones, límites; soporte de sistemas.

- **Medición y Cuantificación del Riesgo.** Considera la cuantificación de los riesgos; la documentación, sustento, variables relevantes de sus metodologías. También los sistemas de Información de riesgos, desempeño de las metodologías, planes de acción en caso de contingencias.

- **Revisión Independiente.** Incluye el rol de la función de auditoria interna en la materia, su independencia y reconocimiento; el alcance, cobertura de sus evaluaciones; la periodicidad de éstas y el seguimiento de planes de acción.

Supervisión del Riesgo Operacional

Esquemáticamente:



Supervisión del Riesgo Operacional

DIRECTORIO

- Definición de Riesgo Operacional.
- Revisión y aprobación de políticas.
- Definición de Tolerancia al Riesgo.
- Mecanismo formal para informarse
  - De la exposición al Riesgo
  - Del cumplimiento de políticas

COMITÉS

- Dispone de comités encargados de riesgo operacional.
- Cumple con el Rol establecido.
- Representante de diferentes áreas.

FUNCIÓN DE RIESGOS

- La función de riesgos es una contraparte efectiva.
- Se encarga del diseño y mantención de un adecuado sistema de identificación, evaluación, seguimiento y control de riesgos.
- Participa en el proceso de definición de Políticas.

Cómo Se Aborda la Supervisión del Riesgo Operacional

POLÍTICAS

- Suficiencia de las Políticas para gestionar todos los ámbitos de la materia.
- Tolerancia al Riesgo.

PROCEDIMIENTOS

- Existencia de Procedimientos compatibles con las Políticas.
- Verificación de su cumplimiento.

Cómo Se Aborda la Supervisión del Riesgo Operacional

METODOLOGÍAS

- Especificas para la Identificación, Evaluación, Seguimiento, Control y Mitigación, en todos los ámbitos del RO.
- Se establecen controles a los Riesgos residuales.
- Se cuenta con sistemas de alertas (monitorear y controlar).

ESPECÍFICAMENTE EN SEGURIDAD

- Se identifican los Activos a Resguardar.
- Se cuenta con un proceso de evaluación de Riesgos que identifique y evalúe las amenazas y vulnerabilidades de los activos.
- Se cuenta con los controles necesarios para Activos Críticos.

Cómo Se Aborda la Supervisión del Riesgo Operacional

- Es independiente de las Áreas Funcionales.
- Dispone de Recursos Suficientes.
- Cubre adecuadamente los diferentes ámbitos del RO.
- Es una función reconocida.

Caracterización Operacional del Banco de Chile

- Es un banco universal, con presencia en todos los ámbitos de negocios. A abril de 2018, ocupaba el 2° lugar en el ranking de colocaciones con una cuota de mercado de 16,32% y concentraba el 15% de los depósitos del sistema bancario, alcanzando el 4° lugar en este ámbito.
- A esa fecha, el banco presenta activos por MMUSD 55,974; colocaciones por MMUSD 43,672; y un patrimonio de MMUSD 5,148.
- Su indicador de adecuación de capital es de 14,2%. Este indicador cumple con lo legalmente requerido y se ubica en los rangos del promedio de la industria (13,6%).

Caracterización Operacional del Banco de Chile

- Cuenta, con una extensa base de clientes, que operan mediante diversos productos y canales, lo que determina un alto nivel de transaccionalidad.

	B. de Chile	Industria	Partic.
N° cuentas corrientes totales	941,007	4,564,696	21%
N° Ctas. Ctes. Persona Natural	802,039	3,958,041	20%
N° Ctas. Ctes. Pesona Jurídica	138,968	606,655	23%
N° Total tarjetas Vigentes	3,777,227	38,538,245	10%
N° T. Crédito Vigentes	1,652,146	13,012,778	13%
N° T. Débito Vigentes	2,125,081	25,525,467	8%
N° T. Crédito C/Movimiento	960,733	5,058,215	19%
N° T. Débito C/Movimiento	998,700	10,564,370	9%
% de T/C C/Movimiento (*)	58%	39%	
% de T/D C/Movimiento (*)	47%	41%	

Caracterización del Banco

- A abril de 2018, posee una red de atención conformada por 397 sucursales (49% ubicadas en la Región Metropolitana), 1.465 cajeros automáticos, una dotación de personal de 11.284 funcionarios y diversos canales no presenciales con creciente y relevante nivel de uso.

Incidente Operacional

- El día jueves 24 de mayo, la institución reportó un incidente que obedeció a una acción cibernética que actuó en días consecutivos. El evento afectó algunos servidores y terminales del personal del banco que operan bajo el sistema operativo *Microsoft Windows.* Esto afectó la normal prestación de los servicios bancarios tanto en sucursales como a través de su *call center.*

- El incidente derivó en la activación de planes de contingencia donde se resolvió desconectar equipos, impactando la operación, fundamentalmente en sucursales, banca telefónica y sistema de pago de alto valor. Para esto último contó con el apoyo del Banco Central de Chile.

Consecuencias del Incidente

Producto de la operación en contingencia se observó:

- Importante degradación del servicio en sucursales, afectando la calidad de la atención a clientes minoristas.
- Hubo efecto contenido en la cadena de pagos, sin embargo se operó en contingencia en operaciones de alto valor.
- No se ha reportado afectación de cuentas o información de clientes.
- El Banco se encuentra en proceso de determinar si hubo afectación de cuentas propias.

Acciones llevadas a cabo por la SBIF

Como es habitual en casos que impactan a una institución relevante del sistema, la SBIF lleva a cabo distintas acciones:

Corto plazo:

- Desde que se conoció el incidente, se tomó contacto con la entidad y se ha establecido un monitoreo permanente.
- Se ha mantenido contacto permanente con las autoridades Banco Central, Ministerio de Hacienda y Comité de Supervisión Financiera.
- Se estableció contacto con otras instituciones financieras con el propósito de advertir la situación y los planes de contingencia ante eventuales contagios.
- Otros contactos: Superintendencia Financiera de Colombia, Proveedores especializados.

Acciones llevadas a cabo por la SBIF

Superintendencia de Bancos e Instituciones Financieras Chile

Mediano Plazo:

- Evaluación de perfeccionamientos normativos.
- Evaluación in situ de la entidad, con objeto de evaluar la gestión efectuada por el banco en el riesgo operacional.
- A nivel país, en el año 2017 se publicó la Política Nacional de Ciberseguridad y la firma del Convenio de Budapest, constituyéndose en un primer paso. Sin embargo, se requiere:
  - **Generar la institucionalidad para la administración de los riesgos y coordinación de los componente críticos a nivel nacional frente a la Ciberseguridad.**
  - **Generar los políticas especificas para la infraestructura critica y coordinar estándares de seguridad y reporte.**
- En este contexto, en enero de 2018 la SBIF emitió una norma especifica relacionada con Ciberseguridad, asumiendo su rol como componente critico en la infraestructura nacional.

Supervisión de la SBIF: Otras acciones

- Adicionalmente, cada vez que existan circunstancias que pudieran impactar la confianza y el riesgo de un banco, la SBIF solicita y revisa los antecedentes. En el caso de riesgo operacional, se orienta a temas que puedan impactar la continuidad del negocio, y la seguridad de la información que puedan a su vez afectar la **reputación** de la institución.

Consideraciones Finales

- La Superintendencia de Bancos e Instituciones Financieras debe velar permanentemente por mantener la estabilidad y solvencia de las entidades fiscalizadas, en resguardo de los depositantes y de la fe pública.

- En ese contexto, toda acción de supervisión se realiza con una lógica prudencial que permita cumplir con estos objetivos.

- Los riesgos tecnológicos y de seguridad de la información, entre los que se encuentran aquellos asociados a la **ciberseguridad**, han adquirido mayor relevancia para la industria bancaria mundial.

- Es por esto que la SBIF ha sido activa en abrir espacios de discusión sobre la materia y en la emisión de instrucciones normativas para que los bancos consideren apropiadamente estos riesgos dentro de sus políticas de gestión (ver actividades).

Consideraciones Finales

- El reciente incidente operacional a nuestro juicio, genera oportunidades de continuar mejorando. En efecto, pueden surgir líneas de trabajo como:
  - Coordinación en la industria bancaria (compartir experiencias).
  - Coordinación con otros actores nacionales.
- Las modificaciones a la LGB, actualmente en discusión en el Senado, ofrecen una oportunidad única para cerrar esta brecha. Es así como, la adopción de los estándares de Basilea III permitirá al supervisor bancario :
  - A través del pilar 1, exigir capital a los bancos para enfrentar pérdidas asociadas a riesgos operacionales.
  - A través del pilar 2, exigir capital por riesgos específicos no cubiertos por el marco general (ejemplo, riesgos cibernéticos derivado de vulnerabilidades en su infraestructura tecnológica).

Presentación Situación Incidente Operacional

Comisión de Economía del Senado

Mario Farren Risopatrón
Superintendente de Bancos e Instituciones Financieras

Junio 2018

Avances de la SBIF en Riesgo Operacional

Superintendencia de Bancos e Instituciones Financieras Chile

Cambios Normativos	Fecha	Alcance
Circular N°3.578	03/2015	Agrega modificaciones al capítulo N°1-7 "Transferencia electrónica de información y fondos" de la RAN, referidas a condiciones mínimas respecto al funcionamiento de **cajeros automáticos** (disponibilidad sobre el 95%, sistemas de monitoreo, etc.).
Circular N°3.579	03/2015	Crea el capítulo N°20-8 "Comunicación inmediata de incidentes operacionales relevantes " de la RAN.
Carta Circular N°1-2016	06/2016	**Seguridad de la Información y Ciberseguridad**: Enfatiza la necesidad de tomar medidas de control, tales como un mayor involucramiento del Directorio en la adopción de mitigadores pertinentes y la realización de evaluaciones periódicas a los sistemas de control.
Circular N°3.612	11/2016	Incorpora norma N°20-9 **"Gestión de la Continuidad del Negocio"** a la RAN, la cual establece lineamientos y buenas prácticas, tales como la adopción de estrategias de administración de la continuidad del negocio, políticas, metodologías y estructuras de gobierno, para una adecuada identificación, cuantificación, evaluación y monitoreo de estos riesgos.
Circular N°3.633	01/2018	Introduce materias específicas de **Ciberseguridad**, dentro de la gestión de riesgo operacional, mediante ajustes en los capítulos N°1-13 "Clasificación de gestión y solvencia" e incorpora el Anexo N° 3 de "Gestión de la Ciberseguridad"; agrega el número 2 al capítulo N°20-8 " de la RAN, con las indicaciones para la generación de la "Base de incidentes de ciberseguridad"; y finalmente incorpora el concepto de ciberseguridad dentro de los "Lineamientos de Educación Financiera".

volver

volver

Avances de la SBIF en Riesgo Operacional

Superintendencia de Bancos e Instituciones Financieras Chile

Hito	Fecha	Alcance
Seminario sobre ciberseguridad (SBIF – Ministerio del Interior)	Mayo de 2016	Medidas que se pueden aplicar para enfrentar la irrupción de cibercrimen en los sistemas de pagos.
Mesa de trabajo público –privada de ciberseguridad (SBIF-ABIF-Ministerio del Interior)	Septiembre de 2016	Enfrentar delitos de clonación de tarjetas y la actualización de medidas de seguridad de cajeros automáticos.
Campaña preventiva (SBIF-ABIF-Ministerio del Interior)	Septiembre de 2016	SBIF, ABIF, Carabineros de Chile y la PDI, difundieron por redes sociales y de manera presencial, un conjunto de medidas preventivas para evitar la clonación de tarjetas en el país.
Seminario sobre ciberseguridad (SBIF y Embajada Británica)	Septiembre de 2016	La actividad (seminario Mind the Gap) se enfocó en los desafíos que representa la visión de ciberseguridad del Reino Unido a partir de la presentación de David Livingstone. Contó además con la participación de Gabriel Bergel, reconocido experto nacional que nos presentó un resumen con su visión de la industria financiera en estas materias.
Pasantía Ciberseguridad Reino Unido	Enero 2017	Reuniones con reguladores y empresas de ciberseguridad: Bank of England, Financial Conduct Authority, CREST, HM Treasury, Control Risk, Level 39, entre otros.
Emisión Norma de Ciberseguridad SBIF	Enero 2018	Norma que incorpora las materias específicas de Ciberseguridad en la Evaluación de Gestión del Riesgo Operacional, particularmente en la definición de la Infraestructura Crítica, considerada en términos de la Política Nacional de Ciberseguridad. Norma que establece la necesidad de que las instituciones bancarias generen una base de incidentes con información estandarizada y completa, de acuerdo a campos establecidos.
Seminario "Fundamentos y Desafíos"	Enero 2018	Seminario de lanzamiento de la Norma de Ciberseguridad SBIF en conjunto con el Ministerio del Interior. El encuentro contó con la participación de la ABIF, para conocer la visión de la industria y del Bancoestado, en su rol de actor clave.