



Superintendencia
de Bancos
e Instituciones
Financieras
Chile

Presentación Ciberseguridad

Comisión de Hacienda 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.
- El mandato de la SBIF se enmarca en la Ley General de Bancos (LGB) y en toda la normativa asociada a ella que ha definido un modelo de supervisión prudencial basado en la gestión de los riesgos.

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 mínimo. Otra normativa es aquella referida a los márgenes de crédito a relacionados y no relacionados del art. 84 de la ley).
- **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.

Normativas impulsadas por la SBIF en Materia de Riesgo Operacional y Ciberseguridad

Cambios Normativos	Fecha	Alcance
Capítulo 1-7 RAN (Circular N°3.578)	03/2015	Se agrega modificaciones al capítulo “Transferencia electrónica de información y fondos” referidas a condiciones mínimas respecto al funcionamiento de cajeros automáticos (disponibilidad sobre el 95%, sistemas de monitoreo, etc.).
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.
Capítulo 20-9 (Circular N°3.612)	11/2016	Se emite norma “ Gestión de la Continuidad del Negocio ”, 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.
Capítulo 20-7 (Circular N°3.629)	12/2017	Establece ajustes al capítulo sobre “Externalización de Servicios”, definiéndose lineamientos de diligencia reforzada que deben establecer las entidades bancarias al externalizar servicios en la modalidad Cloud Computing (Nube) .
Capítulos 1-13 y 20-8 (Circular N°3.633)	01/2018	Introduce en el Capítulo 1-13 “Clasificación de gestión y solvencia”, materias específicas de Ciberseguridad , dentro de la gestión de riesgo operacional y agrega la generación y mantención de una base de incidentes relacionados con la ciberseguridad en el Capítulo 20-8 “Comunicación inmediata de incidentes operacionales relevantes y base de datos de incidentes de ciberseguridad”, de la RAN.

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

Supervisión basada en riesgos:

- El objetivo 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.
- Evitar incidentes operacionales puntuales no es un objetivo de la supervisión basada en riesgos, sino que la reducción de la probabilidad de ocurrencia de dichos incidentes.
- Un adecuado sistema de gestión de riesgo debe permitir mitigar el impacto de un incidente sobre la entidad y la industria.

Nuestra supervisión

Conceptualmente:

- El riesgo operacional es una materia que, en conjunto con otras, la SBIF evalúa en todas las entidades financieras. Esta evaluación incide en la calificación global de la entidad.
- Una mala calificación de la gestión pudiera limitar la incursión de la institución en nuevos negocios.
- Bajo estándares internacionales las pérdidas por riesgo operacional deben ser cubiertas con resguardos patrimoniales.
- Hoy la SBIF no dispone de facultades para realizar requerimientos de capital por riesgo operacional, cuestión que queda abordada en el proyecto de modificación de la Ley General de Bancos, actualmente en tramitación en el Congreso.

Índice de Adecuación de Capital (IAC)

Más y mejor capital

Basilea I

Proyecto de Ley



Basilea III

$$IAC = \frac{K}{APR} \rightarrow \text{Riesgo de Crédito}$$

$$IAC = \frac{K}{APR} \rightarrow \begin{array}{l} \text{Nuevos} \\ \text{Requerimientos} \\ \bullet \text{ Riesgo de Crédito} \\ \bullet \text{ Riesgo Operacional} \\ \bullet \text{ Riesgo de Mercado} \end{array}$$

Basilea III en la LGB

	Acumulado	Composicion	Norma
Pilar 2 entre 0 y 4,0% APR	20,5%	Capital básico o quasi-capital	CMF, con la aprobación de 4/5 de los Comisionados.
Cargo sistémico entre 1,0 y 3,5% APR	16,5%	Capital básico	CMF con informe previo favorable del BCCh
Colchón contracíclico entre 0 y 2,5% APR	13,0%	Capital básico	BCCh con informe previo favorable de la CMF
Colchón de conservación = 2,5%	10,5%	Capital básico	CMF con informe previo favorable del BCCh

T2	T2	8,0%	Bonos subordinados a plazo $\leq 1/2$ CET1, provisionales voluntarias $\leq 1,25\%$ ó 0,625% APR	Características definidas por la CMF con informe previo favorable del BCCh
	AT1	6,0%	Bonos perpetuos convertibles + acciones preferentes $\leq 1/3$ CET1	Características definidas por la CMF con informe previo favorable del BCCh

Cargos de capital y ponderadores en la ley

CET1	Capital básico $\geq 4,5\%$	4,5%	Capital pagado y reservas	Descuentos al capital establecidos por la CMF (puede ser definido por la SBIF)
------	-----------------------------	------	---------------------------	--

Basilea I en Chile

Basilea III

Cargos de capital en la ley y ponderadores definidos por norma

Supervisión del Riesgo Operacional

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 atender 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 las tercerizaciones de sus servicios.

Supervisión del Riesgo Operacional

- **Gestión de procesos:** actividad mediante la 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 contingencias.
- **Revisión Independiente:** Incluye el rol de la función de auditoría 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



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

- Verificar que 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



MEDICION Y
CUANTIFICACION
DEL RIESGO

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



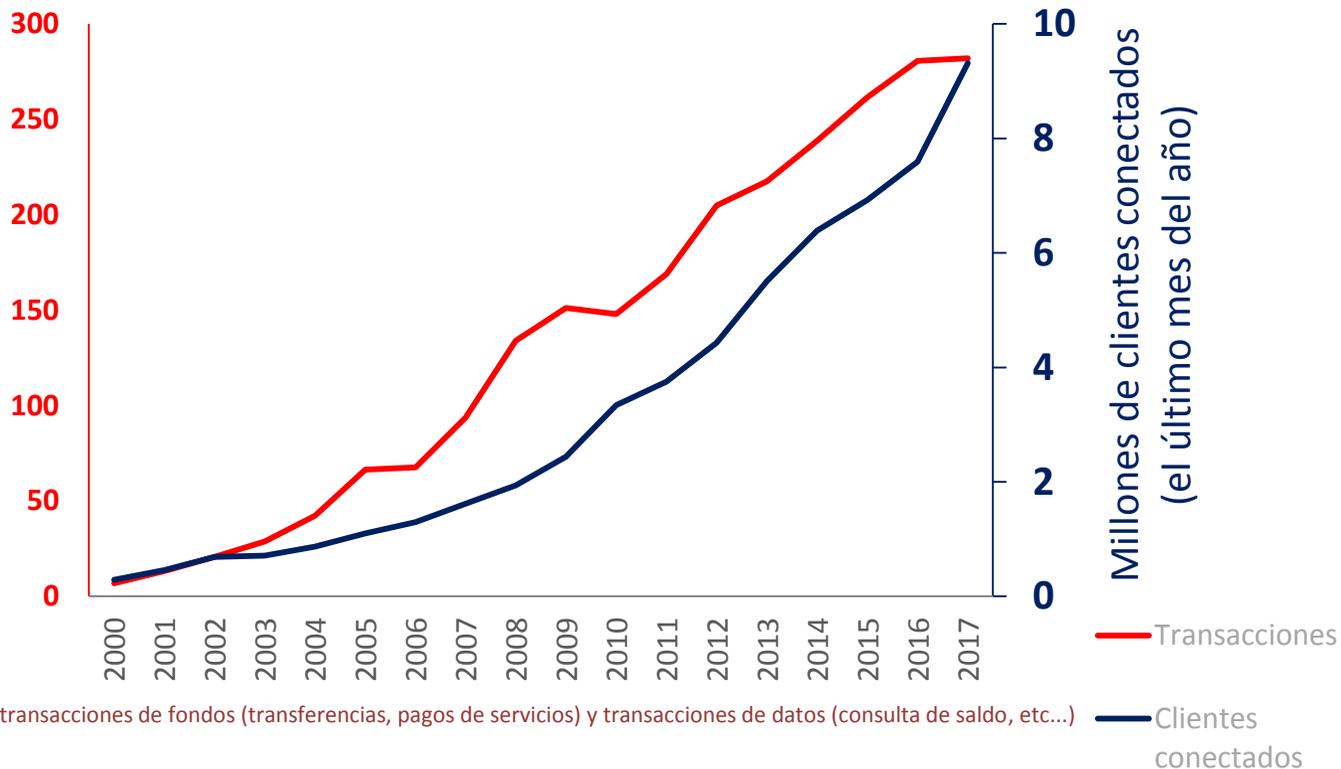
- Es independiente de las Áreas Funcionales.
- Dispone de Recursos Suficientes.
- Cubre adecuadamente los diferentes ámbitos del RO.
- Es una función reconocida.

Los 5 principales riesgos mundiales en términos de probabilidad, según el reporte de Riesgos Globales del WEF

	2017	2018
1	Eventos Climáticos Extremos	Eventos Climáticos Extremos
2	Migración involuntaria a gran escala	Desastres Naturales
3	Grandes Desastres Naturales	Ciberataques
4	Ataques terroristas a gran escala	Fraude o robo de datos
5	Incidente masivo de fraude / robo de datos	Fracaso de la Mitigación y adaptación al cambio climático

Banca por internet: aumento sostenido en el número de clientes conectados y transacciones promedio

Millones de transacciones mensuales promedio *



* se consideran transacciones de fondos (transferencias, pagos de servicios) y transacciones de datos (consulta de saldo, etc...)

Fuente: SBIF

Inversión en TI y Ciberseguridad

(cifras en MM\$)	Total			
	2015	2016	2017	2018 (*)
Inversión en TI	459.256	527.335	596.027	674.304
<i>Indicador 1</i>	<i>6,3%</i>	<i>7,2%</i>	<i>7,7%</i>	<i>8,4%</i>
<i>Indicador 2</i>	<i>13,4%</i>	<i>14,5%</i>	<i>15,8%</i>	<i>17,5%</i>
Inversión en Ciberseguridad	27.161	34.784	38.968	60.961
<i>Indicador 1</i>	<i>0,4%</i>	<i>0,5%</i>	<i>0,5%</i>	<i>0,8%</i>
<i>Indicador 2</i>	<i>0,8%</i>	<i>1,0%</i>	<i>1,0%</i>	<i>1,6%</i>
Protec. Perimetral	4.111	7.631	7.360	17.057
Protec. de Redes	4.555	5.891	6.261	9.370
Protec. de dispo.de acceso a la red	3.983	3.346	3.184	4.155
Protec. de Aplicativos	9.008	10.000	11.837	14.398
Desarrollo de Sistemas	3.503	4.639	5.555	5.507
Capacitación Interna	47	210	109	638
Consultorías	402	224	808	2.267
Otros	1.552	2.844	3.854	7.569
Total Inversión (TI+Ciberseguridad)	486.416	562.120	634.994	735.265
<i>Indicador 1</i>	<i>6,7%</i>	<i>7,7%</i>	<i>8,2%</i>	<i>9,2%</i>
<i>Indicador 2</i>	<i>14,2%</i>	<i>15,5%</i>	<i>16,9%</i>	<i>19,1%</i>
Resultado Operacional Bruto (individual)	7.306.678	7.308.663	7.701.589	8.033.957
Gastos de Apoyo (individual)	3.432.002	3.637.905	3.764.830	3.848.577

Indicador 1 = $\frac{\text{Inversión}}{\text{Resultado Op. Bruto}}$

Indicador 2 = $\frac{\text{Inversión}}{\text{Gastos de Apoyo}}$

Fuente: información preliminar proporcionada por los 17 principales bancos.

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

Corto plazo:

- Se toma contacto con las entidades afectadas y se requiere información de manera permanente.
- Se mantiene contacto permanente con las autoridades ej: Banco Central, Ministerio de Hacienda y Comité de Supervisión Financiera.
- Se establece contacto con otras instituciones financieras con el propósito de advertir las situaciones y los planes de contingencia ante eventuales contagios.
- Otros contactos: otros reguladores y Proveedores especializados en temas de ciberseguridad.
- Otras acciones: Participación en grupos de trabajo especializados.

- Evaluaciones in situ de las entidades, con objeto de verificar la gestión efectuada por el banco en el riesgo operacional.
- Perfeccionamientos normativos. A modo de ejemplo, en enero de 2018 la SBIF emitió una norma específica relacionada con ciberseguridad, asumiendo su rol como componente crítico en la infraestructura nacional.
- Se mantienen reuniones con los gerentes de la industria requiriéndoles definiciones y la comunicación de medidas transversales para fortalecer los niveles de seguridad con que operan sus canales electrónicos,

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.

Otras Actividades de la SBIF en RO.

Hito	Fecha	Alcance
Seminario sobre ciberseguridad (SBIF – Ministerio del Interior)	Mayo de 2016	Medidas que se pueden aplicar para enfrentar la irrupción de ciberdelitos 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 la 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.

Consideraciones Finales

- El objetivo del modelo de supervisión de la SBIF, es que los bancos gestionen adecuadamente los riesgos a que están expuestos, es decir que los bancos identifiquen, midan, controlen y monitoreen adecuadamente los riesgos, desarrollen y gestionen los controles compensatorios necesarios.
- Evitar incidentes operacionales puntuales es un asunto importante, sin embargo la reducción de la probabilidad de ocurrencia de dichos incidentes es el objetivo al que apunta la supervisión basada en riesgos.

Consideraciones Finales

- El reciente incidente operacional a nuestro juicio, genera oportunidades de mejora continua a nivel país y en la industria financiera. En efecto, pueden surgir líneas de trabajo como:
 - Coordinación en la industria bancaria para compartir información y revisar protocolos de seguridad.
 - Coordinación con otros actores nacionales.

Consideraciones Finales

- 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:
 - Exigir capital a los bancos para enfrentar pérdidas asociadas a riesgos operacionales a través del pilar 1.
 - Exigir capital por riesgos específicos no cubiertos por el marco general a través del pilar 2.



Superintendencia
de Bancos
e Instituciones
Financieras
Chile

Presentación Ciberseguridad

Comisión de Hacienda del Senado

Mario Farren Risopatrón
Superintendente de Bancos e Instituciones Financieras

Junio 2018

28

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. Persona 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%	

Nota: Cifras a abril 2018.

Caracterización Operacional del Banco de Chile

- 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 lo que impactó 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.
- Al cierre de mayo el banco constituyó una provisión por MM\$ 8.672, respaldados en una “nota” que indica MM\$ 6.800 por el incidente y MM\$ 1.800 por gastos en asesorías y servicios tecnológicos.

Reclamos de clientes recibidos

- **SBIF:** entre el 24 de mayo al 18 de junio se han recibido 5 reclamos de clientes del Banco de Chile.
- **Banco de Chile:** reporta entre el 24 de mayo y el 14 de junio un total de 48 reclamos.

Nota: El banco al 8 de junio había informado 61 reclamos asociados al incidente, los que en su análisis y gestión posterior se determinó que su origen no se debía a este quedando 45 reclamos. Se adicionan nuevos 3 reclamos al 14 de junio, quedando en total 48 reclamos.