Riesgo Operacional y Ciberseguridad en el Sistema Financiero

Joaquín Vial, Vicepresidente, Banco Central de Chile

Presentación para Comisión de Hacienda del Senado

Banco Central de Chile, Junio 2018

Introducción

- La contención de riesgos operacionales constituye parte integral del marco de gestión de riesgos que pueden afectar al sistema financiero (liquidez, crédito y operacional).

- La sofisticación de los ataques de ciberseguridad experimentados por el sistema financiero internacional en el último tiempo, han aumentado la complejidad de gestión de los riesgos operacionales.

- La gestión de riesgos operacionales históricamente centrada en la continuidad en la provisión de servicios financieros, actualmente incluye aspectos más complejos y sensibles como por ejemplo, pérdidas patrimoniales o de información crítica.

La contención de riesgos operacionales ha aumentado su relevancia sobre la estabilidad del sistema financiero, lo cual forma parte de los objetivos del Banco Central de Chile.

Introducción

- La regulación no puede impedir la ocurrencia de ataques informáticos, pero sí generar condiciones para preverlos y responder adecuadamente si se producen.
- La reforma a la Ley General de Bancos (LGB), en discusión en el Congreso, integra en los requerimientos de capital bancarios cargos adicionales por riesgo operacional, de acuerdo a las orientaciones de Basilea III.
- Para definir estos cargos de capital se confieren al supervisor bancario (SBIF y CMF bajo reforma LGB) facultades amplias de regulación que refuerzan las atribuciones vigentes.
- Los eventos recientes muestran la relevancia de la reforma a la LGB en discusión actualmente en este Congreso.

Respecto del caso reciente que afectó al Banco de Chile, el Banco Central utilizó herramientas a su alcance en el ámbito de sus competencias.

- El jueves 24 de mayo, Banco de Chile informa a primera hora tener inconvenientes para efectuar pagos y solicita al BCCh activar procedimientos de continuidad operacional del Sistema LBTR.

- Este procedimiento permitió habilitar un acceso directo al Sistema LBTR para el Banco de Chile en las dependencias del BCCh (Sala de Contingencia), de acuerdo a las medidas de seguridad establecidas para tal efecto.

- La utilización de este protocolo se extendió hasta el día viernes 25. Los días siguientes, el Banco de Chile accedió al Sistema LBTR desde sus instalaciones.

- Asimismo, como medida adicional para asegurar una mayor cobertura en la liquidación de los pagos, el BCCh decidió extender el horario de cierre del Sistema LBTR desde el 24 de mayo al 01 de junio.

- El día lunes 04 de junio, Banco de Chile inicia su operación normal a las 10:30 hrs.

Para enfrentar este tipo de situaciones el Banco sustenta sus acciones en su rol de preservar la estabilidad financiera y en su modelo de gestión interna

- La responsabilidad del Banco es preservar la continuidad de los sistema de pago y, desde una perspectiva más amplia, la estabilidad del sistema financiero:
  - Advirtiendo o previniendo riesgos que puedan afectar a las entidades del sistema financiero y las infraestructuras que sustentan el funcionamiento de estos mercados.
  - Estableciendo el marco de regulación de los Sistema de Pago de Alto Valor (SPAV), siguiendo estándares internacionales.
  - En el caso particular del Sistema LBTR actúa además como operador y administrador del Sistema.
- El Banco internamente desarrolla y actualiza permanentemente su modelo de gestión de riesgos operacionales, que sustenta sus procesos críticos, incluyendo la operación del Sistema LBTR.

Rol del BCCh en la contención de riesgos operacionales en el sistema financiero

Los riesgos de Ciberseguridad en la estabilidad financiera pueden producirse por:

1. Disrupciones en los servicios financieros de instituciones sistémicas.
2. Potencial pérdida de confianza en la seguridad de los fondos de los depositantes.
3. Ampliación de disrupciones puntuales por la interconexión tecnológica o financieras de entidades del sector.
4. Interrupción de las cadenas de pagos por alguno de los casos anteriores o por fallas en la operación de infraestructura financiera.

A nivel Internacional el riesgo operacional y la ciberseguridad han recibido atención creciente

- **En Basilea II y Basilea III,** se establecen y perfeccionan recomendaciones sobre exigencia de un capital mínimo con fines de riesgo operacional.
- El ***Financial Stability Board*** **(FSB, 2017)** concluye que todas las jurisdicciones pertenecientes han sido activas en abordar la ciberseguridad para el sistema financiero.
- **El mismo reporte concluye que los organismos internacionales** han sido especialmente activos en abordar el tema, publicando guías aplicables a la banca, las infraestructuras del mercado financiero (IMF), empresas, autoridades regulatorias y de supervisión, entre otras.
- Entre las prácticas que las jurisdicciones consideran efectivas para abordar los riesgos de ciberseguridad se encuentran el **seguimiento de estándares y directrices internacionales existentes.**
- **El BCCh es partícipe activo de estas instituciones. Por lo que ha estado siempre actualizado de las orientaciones y recomendaciones en estos temas.**

Para mayor información: FSB (2017) "*Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices".* http://www.fsb.org/wp-content/uploads/P131017-2.pdf

En Chile, las responsabilidades institucionales por el resguardo de la estabilidad financiera son compartidas por el BCCh, CMF, SBIF y CEF

BCCH

- Operador/Regulador de los SPAV: LBTR + CCAV.
- Advierte sobre riesgos de EE.FF. (rol preventivo)
- No tiene facultades de fiscalización .
- Prestamista de última instancia.
- Autorización complementaria ECC.

SBIF

- Fiscalizador y regulador de los bancos (LGB)
- Regulación sobre riesgo operacional y ciberseguridad

CMF

- Fiscalizador y regulador de las Infraestructuras para el Mercado Financiero (IMF)
  - ECC
  - DCV
  - Cámaras de Compensación

CEF

CEF

- Rol de coordinación de supervisores financieros.
- Presidido por el Ministro de Hacienda (2011)
- Grupo de trabajo sobre “Continuidad Operacional”

SPAV: Sistema de Pagos Alto Valor, CCAV: Cámara Compensación de Alto Valor, EEFF: Entidades Financieras, DCV: Depósito Central de Valores, ECC: Entidad de Contraparte Central.

Perspectiva y rol del Banco Central de Chile en el riesgo operacional

Estabilidad Financiera

1	Mandato	Normal funcionamiento de los pagos internos y externos y prestamista de última instancia	Advertir riesgos, promover resguardos y otros elementos de prevención (i.e. Informe de Estabilidad Financiera)
2	Operadores	Rol fundamental en el Sistema de Pagos de Alto Valor	Particularmente del sistema que realiza la Liquidación Bruta y en Tiempo Real (LBTR) de instrucciones de transferencia de fondos
3	Entidad	Como cualquier otra institución que debe velar por su propia continuidad operacional	Marco de Gestión de Riesgo Operacional

La regulación del Sistema de Pagos de Alto Valor (SPAV) se enfoca en su funcionamiento eficiente y seguro, de acuerdo a estándares internacionales.

- Para cumplir su mandato legal de velar por el normal funcionamiento de los pagos, el BCCh cuenta con una serie de atribuciones de regulación aplicables a los SPAV, (art. 35 N° 8 LOC).
- El Banco opera su Sistema de Liquidación Bruta en Tiempo Real (LBTR) para operaciones de pago entre entidades bancarias.
  - Dicta la reglas que deben cumplir sus participantes (bancos), lo cual incluye estándares tanto operacionales como financieros.
  - Aplica los máximos estándares de gestión en todos los componentes que debe administrar internamente para permitir el funcionamiento eficiente y seguro de LBTR.
- Para el segundo componente de los SPAV, correspondiente a la Cámara de Compensación de Alto Valor (actualmente administrada por Combanc S.A.), el Banco define su regulación, sujeta a la fiscalización de la SBIF.
- Principales componentes de los Sistemas de Pago de alto y bajo valor (Anexo 1)

La regulación del Sistema de Pagos de Alto Valor (SPAV) se enfoca en su funcionamiento eficiente y seguro, de acuerdo a estándares internacionales.

- Los SPAV son parte de las Infraestructuras necesarias para el funcionamiento de los mercados financieros (IMF, por sus siglas en inglés).
- Las otras IMF, corresponden a:
  - Entidades de Contraparte Central (ECC) y Cámaras de Compensación de Valores, reguladas a través de la Ley 20.345, supervisada por la CMF (CMF y Banco Central aprueban sus normas de funcionamiento).
  - Depósito Central de Valores, sujeta exclusivamente a la fiscalización y regulación de la CMF.
- En enero de 2018, el BCCh requirió a los SPAV el cumplimiento y evaluación periódica de los Principios para las Infraestructuras del Mercado Financiero (PFMI).
  - Los PFMI establecen estándares mínimos de gestión de riesgo a través de todas las infraestructuras a nivel internacional.

Para mayor información: CPMI-IOSCO (2012) “Principios aplicables a las Infraestructuras del Mercado Financiero” https://www.bis.org/cpmi/publ/d101_es.pdf

El BCCh cuenta con un marco de gestión de riesgos, aplicable a todos sus sistemas críticos incluyendo al Sistema LBTR

- El BCCh cuenta con:
  - Política de Gestión Integral de Riesgo
  - Requerimientos de funcionamiento bajo estándares internos, planes y procedimientos de continuidad operacional.
- En este marco el Banco ha establecido internamente una estrategia focalizada en materias de Ciberseguridad.
- El sistema LBTR está sujeto a procedimientos e instancias de control interno en concordancia con la Política Integral de Gestión de Riesgos del Banco, en cuanto éste actúa como ente normativo, propietario y administrador de dicho Sistema.
- El sistema LBTR cuenta con regulaciones específicas que establecen procesos de contingencia y continuidad operacional (Capítulos III.H.4 y III.H.4.1 del CNF BCCh) así como Procedimientos de Continuidad Operacional para sus Participantes.

Para estos efectos el BCCh organiza controles de Ciberseguridad, sobre la base de niveles de control

1	Nivel de Inteligencia	Suscrito a fuentes de inteligencia como FS-ISAC, parte del grupo liderado por el BCE, grupo BIS, reuniones CEMLA y diversos proveedores internacionales
2	Nivel de Prevención	Cultura, simulaciones, clasificación de información altamente sensible, mecanismos de dos o tres autorizadores
3	Nivel de Protección	Soluciones tecnológicas de control a nivel Perimetral, Red y Equipos
4	Nivel de recuperación	Ejercicios de contingencia y recuperación de manera periódica , Data Centers alternos

Conclusiones y Desafíos pendientes

Los desafíos que se avizoran de mayor urgencia corresponden a los siguientes:

- Los ataques cibernéticos van a seguir ocurriendo (no pueden evitarse completamente), ellos van evolucionando y de esa forma desafiando nuevos sistemas de protección. Esta dinámica sugiere una atención permanente de reguladores, supervisores y del sector privado.
- Es especialmente relevante aumentar la resiliencia del sistema bancario frente a eventos de disrupción tecnológica. En lo más inmediato, el proyecto de nueva LGB permite ponerse al día con estándares internacionales en el tratamiento de riesgo operacional.
- El eslabón más débil en la cadena de seguridad son las personas. Los “errores humanos” son una puerta de entrada para los ataques. Esta situación advierte sobre la importancia de avanzar con un cambio cultural al interior de las organizaciones y también en los usuarios del sistema financiero.
- Las infraestructuras del mercado financiero son fundamentales para el buen funcionamiento del sistema de pagos. La seguridad y estabilidad de las plataformas digitales de dichas infraestructuras involucra a todos los actores que participan en ellas.

Los desafíos que se avizoran de mayor urgencia corresponden a los siguientes:

- En este contexto, es necesaria una colaboración regular y eficiente entre los actores del sistema —bancos e instituciones financieras, reguladores y supervisores, y el BCCh.
- Existen cuatro niveles fundamentales de acción señalados anteriormente en declaraciones del Presidente del Banco: inteligencia, prevención, protección y gestión de contingencias/recuperación. Esta colaboración todavía puede y debe ser mejorada.
- Un paso importante en esta dirección es la firma del Memorándum de Entendimiento en el Consejo de Estabilidad Financiera, respecto a continuidad operacional, para fines de reforzar el intercambio de información y la acción coordinada conjunta.
- A su vez, el país debe avanzar en modernización de legislación de delitos informáticos (Ley Actual es de 1993).

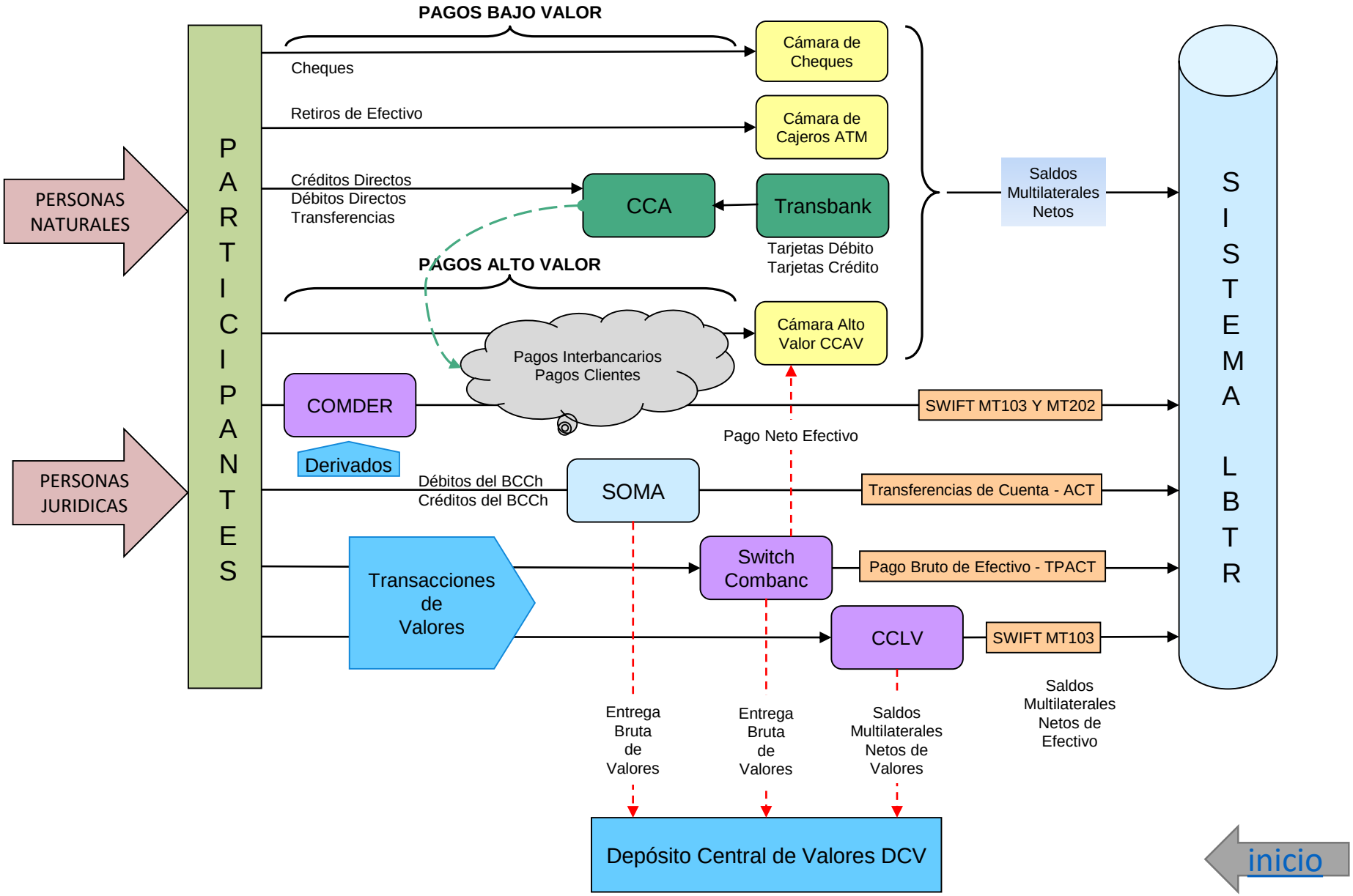
Riesgo Operacional y Ciberseguridad en el Sistema Financiero

Joaquín Vial, Vicepresidente, Banco Central de Chile

Presentación para Comisión de Hacienda del Senado

Banco Central de Chile, Junio 2018

Funcionamiento de los Sistemas de Pago (alto y bajo valor) y su interacción con las principales IMF en Chile



inicio