RECUADRO I.1
CIBERSEGURIDAD Y ESTABILIDAD FINANCIERA

La contención de los riesgos operacionales en el sector financiero representa una preocupación tanto para los reguladores como para la industria. Típicamente, los mecanismos de contención de estos riesgos consideran la adopción de medidas para mitigar los efectos negativos de eventos como desastres naturales, disrupciones en las infraestructuras físicas y tecnológicas, así como ataques cibernéticos.

En los últimos años los riesgos asociados a la ciberseguridad han adquirido mayor relevancia. Lo anterior se relaciona con la creciente sofisticación, mayores niveles de tecnología en sus procesos e interconexión de las entidades financieras. En este sentido, si bien los riesgos cibernéticos tienen en común con otros riesgos operacionales el potencial de afectar la continuidad de los servicios financieros, pueden implicar riesgos de mayor alcance para la estabilidad financiera, por ejemplo, al involucrar robos de activos financieros o de información que puedan comprometer más directamente a las entidades víctimas de este tipo de ataques.

En los últimos años, diversas jurisdicciones reportan cada vez con mayor frecuencia vulneraciones a la ciberseguridad de instituciones financieras, con consecuencias materiales en varios casos. A modo de referencia, el ciberataque a tres bancos en Corea del Sur en 2013, alteró información sensible, operaciones monetarias y funcionamiento de cajeros automáticos; el Banco Central de Bangladesh sufrió en 2016 el robo de 81 millones de dólares; en India, el 2016 los bancos sufrieron una filtración que comprometió información de 3,2 millones de tarjetas de créditos; y en abril de este año tres bancos fueron atacados en México, lo que resultó en disrupciones en sus servicios y en pérdidas patrimoniales. A nivel local, el ciberataque sufrido por el Banco de Chile el pasado 24 de Mayo, así como el informado el 6 de noviembre por Banco Consorcio, demuestran que nuestro sistema financiero no está exento de estos eventos (Capítulo VI).

Estabilidad financiera

Existen al menos cinco casos donde la materialización de riesgos de ciberseguridad puede amenazar la estabilidad financiera. Primero, los ciberataques pueden causar disrupciones en los servicios financieros de las instituciones afectadas, ya sea bancos o infraestructuras financieras. Debido a las interconexiones entre estas entidades, las disrupciones eventualmente se podrían propagar al resto del sistema financiero. Segundo, los ciberataques pueden interrumpir el normal flujo de pagos, afectando a las demás instituciones, incluidas las infraestructuras del mercado financiero, a través del sistema de pagos de alto valor (SPAV). En su origen, estos dos canales se relacionan mayormente con la tradicional concepción de ciberseguridad como riesgo operacional. Tercero, un ciberataque puede generar pérdidas de información crítica para el sistema financiero, incluyendo información sensible de los clientes. Cuarto, pueden debilitar la situación patrimonial de una institución financiera como consecuencia de un robo de sus recursos. Quinto, un ciberataque puede mermar la confianza de los agentes en la seguridad del sistema financiero. Por ejemplo, un ciberataque a los sistemas de pago de bajo valor, merma la confianza de los participantes inhibiendo las transacciones y últimamente afectando a la actividad financiera.

Por cierto, el impacto sobre la estabilidad financiera dependerá de factores como la magnitud del ataque, el tamaño de las instituciones afectadas y su capacidad de respuesta para retomar su funcionamiento normal.

Rol del Banco Central de Chile

El rol del Banco Central de Chile frente al tema de ciberseguridad está determinado por dos elementos centrales: (i) Su mandato legal de velar por el normal funcionamiento de los pagos, y (ii) Su responsabilidad por la gestión y administración directa de procesos críticos para el sistema financiero.

Según el mandato establecido en su Ley Orgánica Constitucional, el BCCh debe velar por el normal funcionamiento de los pagos internos y externos, debe asegurar la provisión de liquidez en tiempos normales y además tiene el rol de prestamista de última instancia. Estas atribuciones se traducen en una preocupación permanente por la estabilidad del sistema financiero y se materializan en acciones concretas. Primero, el BCCh a través del Informe de Estabilidad Financiera, u otros canales, advierte

riesgos al mercado y, a través de instancias como el Consejo de Estabilidad Financiera (CEF), promueve resguardos necesarios. Segundo, tiene una participación en la regulación del sistema financiero, a través de la cual incide, por ejemplo, sobre los estándares de gestión de los riesgos (liquidez y mercado) y sobre las condiciones de participación del sector bancario, el mercado de derivados y captaciones. Además tiene un rol de regulador de las infraestructuras del mercado financiero y del SPAV. Por último, provee de liquidez de forma permanente al sistema interbancario.

En paralelo, el BCCh debe gestionar la continuidad operacional de diversos procesos críticos para el sistema financiero que el Banco administra. Así, el Banco debe gestionar activos financieros en el exterior, como lo son sus reservas internacionales o los fondos soberanos que administra por encargo del Ministerio de Hacienda. Adicionalmente, el banco administra y genera información estadística y financiera fundamental y sensible para el sistema. Por último, es el operador del Sistema de Liquidación Bruta en Tiempo Real (LBTR), que liquida los pagos entre instituciones financieras y por ende tiene responsabilidad directa frente a disrupciones operacionales que puedan afectarlo[1/].

Coordinación institucional y desafíos futuros

Además del BCCh, otras autoridades tienen un importante rol en la fiscalización y regulación del sistema financiero, incluyendo la banca (SBIF), valores e infraestructuras del mercado financiero (CMF) y fondos de pensiones (SP). En lo más reciente, algunas de estas autoridades han publicado recomendaciones e incorporado en la normativa cambios relativos al resguardo de la ciberseguridad (Capítulo V).

Considerando la naturaleza de los riesgos de ciberseguridad, su contención involucra a diversas autoridades del país, incluyendo por ejemplo a las policías expertas en la prevención y contención de delitos financieros, lo cual supera el alcance de las autoridades y entidades que conforman directamente al sistema financiero.

En el ámbito propiamente financiero, y considerando que la experiencia internacional sugiere que los ataques cibernéticos pueden tener un efecto sistémico, se requieren acciones coordinadas y consistentes de las autoridades que cuentan con atribuciones y responsabilidades en este ámbito. En este sentido el CEF, de acuerdo a su rol en la coordinación y articulación de políticas conjuntas de los supervisores financieros, reactivó el Grupo de Trabajo de Continuidad Operacional del CEF (GCOCEF), lo que derivó en la firma de un Memorándum de Entendimiento con el fin de diseñar e implementar un protocolo de contingencia para problemas de riesgos operacionales causados por disrupciones a la ciberseguridad. Asimismo, el CEF solicitó una asistencia técnica al FMI en estas materias.

En este contexto, el poder Ejecutivo anunció un proyecto de ley de Ciberseguridad Financiera, que a su vez es parte de la estrategia general del Gobierno para el fortalecimiento de la Ciberseguridad. Según lo señalado por el Ministerio de Hacienda, el proyecto incluirá mandatos y atribuciones inequívocas y uniformes para todas las autoridades; exigencias proporcionales al potencial impacto de la entidad financiera sobre el sistema; obligación de reportar continuamente a las autoridades sobre gestión e incidentes específicos; y elaboración de evaluaciones de riesgo, planes de contingencia, capacitación en ciberseguridad y realización de pruebas, entre otros temas.

Algunos de los desafíos a futuro para los reguladores son revisar, con miras a perfeccionar, el marco regulatorio y de supervisión en materia de gestión de riesgo operacional y ciberseguridad. Lo anterior puede incluir la incorporación de un mayor grado de detalle en las normas, de manera de disminuir discrecionalidad en implementación de medidas; graduación de requisitos de acuerdo a estándares y mejores prácticas internacionales; y la consideración de riesgos transversales e impactos en otras instituciones.

Por otra parte, se debe mejorar el seguimiento y monitoreo de los riesgos de ciberseguridad. Lo anterior implica el análisis de nuevas métricas que permitan una correcta identificación y ponderación de estos riesgos. Asimismo, se debe evaluar si las capacidades de supervisión de estas materias son las adecuadas, o bien deberían ser perfeccionadas o creadas.

Por último, es fundamental que las entidades financieras del sector privado revisen de manera permanente si los riesgos de ciberseguridad a los que están expuestos están bien administrados. Ello, ya que no sólo son responsables frente a sus clientes por los compromisos que adquirieron con ellos, sino que además forman parte de un sistema altamente interconectado. Por lo demás, está en su propio interés resguardar adecuadamente sus recursos e información, puesto que la materialización de estos riesgos tiene costos patrimoniales y reputacionales que pueden ser elevados.

[1/] Recientemente, como parte de un proceso de actualización de su estructura gerencial, el BCCh creó el cargo de Jefe de Ciberseguridad, el que estará encargado de monitorear los riesgos informáticos que enfrenta la institución.