RECUADRO II.2:

Ciberseguridad en el sistema financiero y de pagos

La ciberseguridad comprende el conjunto de medidas destinadas a proteger la confidencialidad, integridad, disponibilidad y autenticidad de la información, así como también los sistemas y servicios digitales frente a amenazas o incidentes (BCCh, 2018; FMI, 2026; FSB, 2023a). En el sistema financiero y de pagos, estos riesgos son especialmente relevantes por la alta intensidad de uso de datos, la interconexión entre instituciones, la dependencia tecnológica y la necesidad de asegurar la continuidad operacional de servicios críticos. La afectación de cualquiera de estos atributos puede generar costos económicos, reputacionales y operacionales, o incluso afectar la confianza en el sistema. Por eso, la ciberseguridad ha pasado de ser un desafío tecnológico a un componente esencial para la resiliencia del sistema financiero.

La relevancia de este tema se refleja en las orientaciones de organismos internacionales para prevenir, monitorear y recuperarse de incidentes. Desde 2019, el Fondo Monetario Internacional (FMI) ha cubierto temas de ciberseguridad en su Programa de Evaluación del Sector Financiero (FSAP) y en su Global Financial Stability Report. Adicionalmente, se observa un aumento en las solicitudes de asistencia técnica formuladas por diversos países al FMI en esta materia (FMI, 2026). Por su parte, el Financial Stability Board (FSB) ha avanzado en materia de resiliencia operacional, taxonomía, reportes de incidentes y gestión de riesgos de terceros (FSB, 2023a, FSB, 2023b).

El BCCh, como regulador, operador y procesador de información, realiza un seguimiento permanente de los riesgos operacionales y de ciberseguridad. En su rol regulador, el Banco mantiene una revisión continua de las disposiciones de su Compendio de Normas Financieras aplicables a los sistemas de pago y sus participantes (BCCh). Como operador del Sistema LBTR, el BCCh dispone de protocolos y procedimientos internos alineados con la Política de Gestión de Riesgos institucional y cuenta con un Departamento de Ciberseguridad encargado de definir directrices para el referido Sistema, cuyo grado de observancia de los estándares internacionales determinados por CPMI-IOSCO se reporta públicamente[1]/. Finalmente, como receptor y procesador de estadísticas, el BCCh cuenta con políticas de seguridad de la información y resiliencia operacional que son constantemente revisadas.

Por su parte, la CMF cuenta con normativa, en el ámbito de sus atribuciones, sobre gestión de seguridad de la información y ciberseguridad. Esta normativa establece exigencias para bancos, filiales, sociedades de apoyo al giro y emisores y operadores de tarjetas de pago. Entre los elementos relevantes se encuentran el involucramiento del directorio, registro y gestión de incidentes, estándares de control de seguridad de la información y requerimientos para empresas a las que se externalizan servicios.

La Ley de Ciberseguridad define un nuevo marco institucional y obligaciones a los participantes del sistema financiero. Esta ley crea la Agencia Nacional de Ciberseguridad (ANCI) y fija estándares de prevención,

[1]/ Entre otras materias, las directrices consideran el establecimiento de procedimientos de acceso, como el uso de la red privada del Banco, la asignación y administración de roles y perfiles, la verificación de identidad de los usuarios, y la protección en las comunicaciones. El marco de divulgación sobre la observancia de los principios aplicables a las Infraestructuras del Mercado Financiero de CPMI-IOSCO del Sistema LBTR se publica anualmente.

reporte y resolución de incidentes para la banca, entidades de servicios financieros y de pago, según corresponda, infraestructuras del mercado financiero, entre otras.

La permanente preocupación por la ciberseguridad de los reguladores y la industria financiera ha adquirido nueva relevancia ante los desarrollos tecnológicos recientes. A nivel global, la mayor digitalización e interconexión de los servicios financieros, junto con la creciente sofisticación de las amenazas, incluidas aquellas potenciadas por Inteligencia Artificial (IA), han reforzado la dimensión sistémica del riesgo cibernético. En línea con esta preocupación, el Bank for International Settlements (BIS) publicó un análisis sobre los riesgos cibernéticos asociados al uso de modelos avanzados de IA y sus potenciales implicancias para la resiliencia de las infraestructuras del mercado financiero (BIS, 2026). A ello se suman la dependencia de proveedores tecnológicos críticos (especialmente de servicios en la nube), las tensiones geopolíticas y el avance de la computación cuántica. Internacionalmente, se ha observado un incremento en la frecuencia y el costo de los ciberincidentes en el sector financiero, siendo los bancos los principales afectados (FMI, 2026). A nivel local, estimaciones de la industria indican que el sector financiero es de los más expuestos a amenazas, varias de ellas potenciadas por inteligencia artificial y otras herramientas utilizadas para cometer fraude, lo que ha elevado la preocupación de autoridades como el BCCh y la CMF[2]/.

Los desarrollos recientes refuerzan la necesidad de abordar la ciberseguridad como un componente de la resiliencia del sistema financiero, y no solo como un riesgo tecnológico interno de cada institución. La continuidad de los servicios financieros depende de la capacidad de las entidades para prevenir, detectar, contener y recuperarse de incidentes, así como de la resiliencia de sus proveedores tecnológicos, redes de comunicaciones, servicios digitales y otras dependencias críticas. En un ecosistema altamente interconectado, una vulnerabilidad en un proveedor externo puede amplificar el impacto de un incidente más allá de la entidad directamente afectada. Por ello, el BCCh, en coordinación con las demás instituciones reguladoras y supervisoras financieras, así como con la institucionalidad de ciberseguridad vigente, continuará monitoreando la evolución de estos riesgos y revisando sus políticas y protocolos de coordinación, con el fin de contribuir a la resiliencia del sistema.

[2]/ Por ejemplo, en abril de este año, tras advertencias de autoridades económicas de Estados Unidos a grandes bancos respecto de los riesgos asociados al modelo Claude Mythos de Anthropic, la CMF informó que se encontraba monitoreando la posible exposición de sus supervisados, en coordinación con la Agencia Nacional de Ciberseguridad. Por su parte, el BCCh ha señalado los potenciales riesgos asociados a la ciberseguridad no solo en diversos Informes de Estabilidad Financiera (IEF), sino que también en las presentaciones ante el Senado. Por ejemplo, el segundo semestre de 2022 el IEF se refirió al riesgo operacional, mientras que el del primer semestre de este año abordó los riesgos asociados a la IA.