Riesgo cibernético: Una preocupación creciente para la estabilidad macrofinanciera

Con la digitalización en auge, las tecnologías en evolución y las tensiones geopolíticas en aumento como telón de fondo, los incidentes cibernéticos, en particular los malintencionados, se han tornado más frecuentes en las dos últimas décadas, y sobre todo desde 2020. Incidentes serios en instituciones financieras importantes podrían amenazar la estabilidad macrofinanciera al provocar pérdida de confianza, perturbaciones en servicios críticos y efectos de contagio en otras instituciones debido a interconexiones tecnológicas y financieras.

Este capítulo concluye que, si bien hasta la fecha los incidentes cibernéticos no han tenido repercusiones sistémicas, el riesgo de cuantiosas pérdidas directas —como mínimo de USD 2.500 millones— para las empresas debido a ese tipo de incidentes sí ha aumentado. Más aún, las pérdidas indirectas resultantes de los incidentes cibernéticos también son significativas y tienden a situarse en niveles superiores a los de las pérdidas directas declaradas por las empresas.

Comprender los factores que contribuyen tanto a los incidentes cibernéticos como a su prevención es fundamental para desarrollar políticas y estrategias robustas de seguridad cibernética. El análisis que se realiza en el capítulo indica que la digitalización y las tensiones geopolíticas incrementan de modo significativo el riesgo de incidentes cibernéticos mientras que, por otro lado, una legislación más desarrollada sobre seguridad cibernética y una mejor gobernanza cibernética contribuyen a mitigar ese riesgo.

El sector financiero está muy expuesto a los riesgos cibernéticos, como ilustra el hecho de que una quinta parte de todos los incidentes afecten a compañías financieras. La alta concentración de mercado y la baja sustituibilidad, sobre todo si se consideran servicios críticos como los de pago y custodia bancaria, podrían hacer que los incidentes cibernéticos en instituciones financieras resultaran particularmente perturbadores, lo cual destaca la importancia de reforzar la seguridad cibernética y la resiliencia operativa. Las operaciones de las instituciones financieras a menudo dependen de proveedores externos de servicios informáticos, lo que también incrementa el riesgo de que shocks adversos comunes generen contagio con efectos sistémicos.

Un incidente cibernético grave en una institución financiera puede disminuir la confianza en el sistema financiero en su conjunto y, en casos extremos, llevar a liquidaciones masivas de posiciones en el mercado e incluso a corridas y pánicos bancarios. Aunque todavía no se ha producido ninguna corrida bancaria significativa debido a un ataque cibernético, el análisis empírico indica que ataques cibernéticos sí han causado modestas —pero hasta cierto punto persistentes— salidas de depósitos en bancos estadounidenses pequeños.

En vista de que el sistema financiero mundial se enfrenta a riesgos cibernéticos significativos y crecientes, los marcos de políticas y gobernanza deben actualizarse constantemente para adecuarse a las circunstancias cambiantes. No obstante, los resultados de un estudio de bancos centrales y autoridades de supervisión en mercados emergentes y economías en desarrollo indican que los marcos de política de seguridad cibernética son todavía inadecuados e insuficientes.

La resiliencia cibernética del sector financiero debería aumentar con el desarrollo de estrategias nacionales de seguridad cibernética adecuadas, marcos de regulación y supervisión apropiados, una fuerza de trabajo capacitada en materia de seguridad cibernética y acuerdos nacionales e internacionales de intercambio de información. Para facilitar un seguimiento más eficaz de los riesgos cibernéticos habría que reforzar los intercambios de información sobre incidentes cibernéticos. Los supervisores deberían exigir a los miembros de los directorios de las empresas que rindan cuentas en cuanto a la gestión de la seguridad cibernética de las instituciones financieras y la promoción de una cultura del riesgo adecuada, la "higiene" cibernética y la capacitación y sensibilización en materia cibernética. Para limitar las potenciales perturbaciones resultantes de incidentes cibernéticos, las instituciones financieras deberían formular y poner a prueba procedimientos de respuesta y recuperación ante ataques, y las autoridades nacionales deberían desarrollar protocolos de respuesta y marcos de gestión de crisis eficaces.

El FMI ayuda de forma activa a que los países miembros consoliden sus marcos de seguridad cibernética a través de Programas de Evaluación del Sector Financiero e iniciativas para el fortalecimiento de las capacidades. La versión íntegra del informe en inglés puede consultarse en: http://IMF.org/GFSR-April2024.