Recuadro 7
RIESGO CIBERNÉTICO: RELEVANCIA Y ENFOQUES PARA SU REGULACIÓN Y SUPERVISIÓN

Felipe Clavijo Ramírez
Daniel Osorio
Eduardo Yanquen*

Durante los últimos años el mundo financiero ha sido testigo del desarrollo vertiginoso de tecnologías innovadoras en el área de los servicios financieros, las cuales han resultado en nuevos modelos de negocio y nuevos procesos o productos. Según el Financial Stability Board (FSB, 2017a), el desarrollo e implementación de estas tecnologías puede llegar a generar múltiples e importantes beneficios para la estabilidad financiera (e. *g.*: descentralización, diversificación, eficiencia, transparencia y mayor inclusión financiera), pero al mismo tiempo propiciaría la generación de nuevos riesgos. El FSB divide estos riesgos en dos categorías: microfinancieros y macrofinancieros. Dentro de la primera clasificación se incluye el riesgo cibernético, el cual es el tema central del presente recuadro.

1. ¿Qué es el riesgo cibernético y por qué es relevante para la estabilidad financiera?

Según el Instituto de Gestión de Riesgos (Institute of Risk Management), organismo líder a nivel mundial en todo lo que compete a la gestión de los riesgos que enfrentan las empresas, el riesgo cibernético se define como cualquier riesgo de pérdida financiera, afectación o daño de la reputación de una organización derivado de algún tipo de falla de sus sistemas tecnológicos de información. El FSB (2017a) clasifica al cibernético como un riesgo microfinanciero de carácter operativo, debido a que puede surgir de fallas en los sistemas de información, error humano o influencias externas.

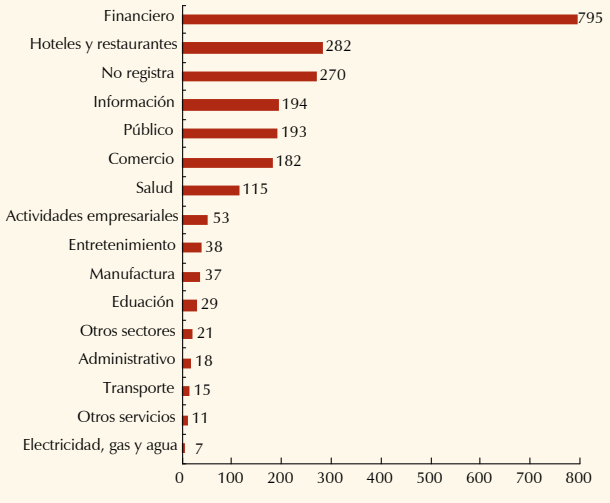
La forma más común como se ha materializado el riesgo cibernético en años recientes ha sido mediante lo que se conoce como ataques cibernéticos. En esencia, estos son acciones ilegales realizadas por *hackers,* con el objetivo principal de obtener cierto beneficio, al generar daños en los sistemas tecnológicos de una organización, dominarlos o robar información contenida en ellos. A raíz del desarrollo de nuevas tecnologías y soluciones digitales, la exposición de las entidades al riesgo cibernético se ha incrementado, debido a que estas innovaciones han expandido el rango y el número de puntos de entrada que los *hackers* pueden atacar en busca de deficiencias o debilidades en los sistemas.

De acuerdo con el Fondo Monetario Internacional (FMI, 2017), existen dos tipos de costos asociados a los ataques cibernéticos. Por un lado, están los costos directos, que incluyen investigaciones forenses, asesoría legal, notificaciones al cliente, protección y seguridad al consumidor, y medidas posataque para mitigar sus efectos. Por otro lado, se encuentran los costos indirectos, los cuales son menos visibles, con efectos de más largo plazo y más difíciles de cuantificar *exante*. En esta categoría se enmarcan los efectos adversos sobre la marca de la institución afectada (riesgo reputacional), la depreciación del valor de la propiedad intelectual, mayores gastos operacionales para prevenir futuros ataques y el impacto sobre las primas que paga el afectado para asegurarse contra futuros eventos. Según el FMI (2017), el 90% de los costos derivados de incidentes cibernéticos es atribuible a factores indirectos.

En el ámbito internacional se ha podido evidenciar que, en los últimos años, los ataques cibernéticos se han intensificado contra las infraestructuras financieras. Esto es preocupante debido a que estos ataques tienen el potencial de propagarse y ser sistémicos. De acuerdo con una encuesta realizada por Verizon (2016), la industria financiera fue la más afectada en 2015 por este tipo de incidentes (Gráfico R7.1).

Algunos ejemplos recientes que han prendido las alarmas en la industria financiera sobre los efectos de los ataques cibernéticos, debido a la importancia de las instituciones afectadas y la magnitud de las pérdidas incurridas, sucedieron en Rusia, Bangladesh y Ecuador. En septiembre de 2014 *hackers* lograron acceder al sistema electrónico de negociación de

Gráfico R7.1
Número de ataques cibernéticos en 2015 con pérdida confirmada de información, por sector económico



Fuente: Verizon (2016).

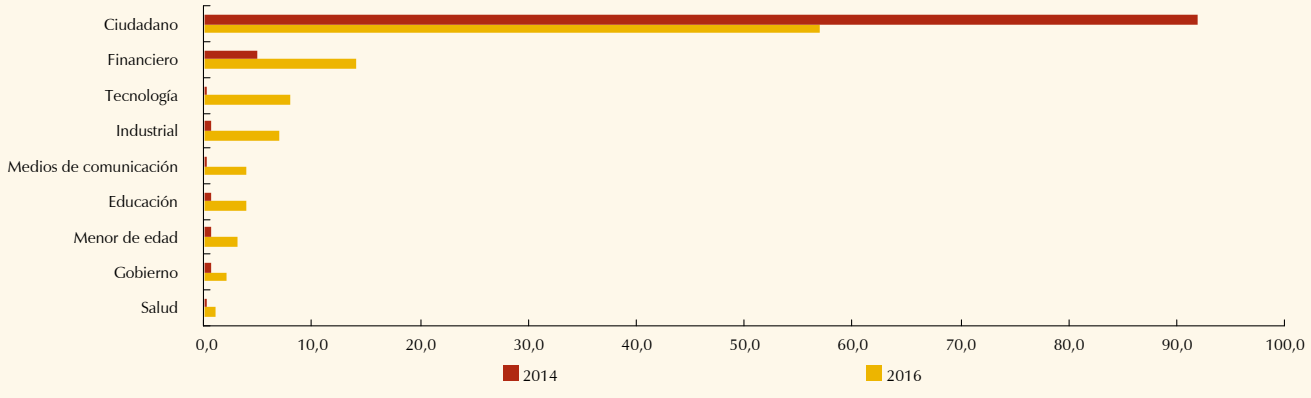
* Los autores pertenecen al Departamento de Estabilidad Financiera del Banco de la República. Sus opiniones no comprometen al Banco de la República ni a su Junta Directiva. Los errores u omisiones que persistan son responsabilidad exclusiva de los autores.

divisas de un banco comercial ruso utilizando un *software* malicioso denominado Corkow. Meses después, en febrero de 2015, ejecutaron en tan solo catorce minutos numerosas transacciones por un valor total de USD 400 millones (m), las cuales causaron una volatilidad anormal en la tasa de cambio del rublo frente al dólar (FMI, 2017). Posteriormente, durante 2016 un grupo de *hackers* logró robar USD 31,0 m del banco central de ese mismo país, de los cuales las autoridades solo lograron recuperar USD 26,0 m. El método que utilizaron fue la falsificación de las credenciales de los clientes del banco e inicialmente planeaban robar más de USD 86,0 m[1]. Por su parte, en Bangladesh, en febrero de 2016 criminales cibernéticos robaron USD 81,0 m al banco central plantando un virus en el servidor, el cual permitió a los *hackers* ordenar transferencias por cerca de USD 1,0 billón (algunos de los mensajes fueron cancelados debido a un error tipográfico; véase FMI, 2017). Finalmente, en mayo de 2016 en un banco ecuatoriano, el Banco del Austro, atacantes utilizaron un método similar para robar USD 12,0 m y transferirlos a distintas cuentas en todo el mundo[2].

Además del robo de recursos, los bancos se enfrentan al riesgo del robo de información. Uno de los primeros incidentes de este tipo se registró en Corea del Sur en marzo de 2013. Tres bancos fueron víctimas de ataques cibernéticos que borraron archivos de su sistema de información e interrumpieron transferencias de dinero y el funcionamiento de los cajeros electrónicos, infectando 48.000 computadores y causando una pérdida total estimada en USD 738,0 m (FMI, 2017). Otro incidente ocurrió cuando un grupo de *hackers* robó datos de cien millones de clientes de JP Morgan Chase durante tres años, hasta ser descubiertos a finales de 2015[3]. El Banco Central de Catar también fue víctima de estos ataques, cuando en 2016 enfrentó el robo de documentos que fueron difundidos en las redes sociales y que incluían archivos corporativos confidenciales e información financiera de sus clientes[4]. Por otro lado, el banco suizo BCGE sufrió un ataque que reveló 30.192 correos relacionados con comunicaciones privadas con sus consumidores[5]. El más reciente ha sido el caso del ente regulador financiero polaco que vio comprometidos sus servidores en un ataque ocurrido a principios de 2017. Los atacantes expusieron archivos que los bancos polacos utilizan para reportar información con fines de supervisión, afectando así a toda la industria[6].

En Colombia, al igual que en el entorno internacional, el crimen cibernético contra instituciones del sistema financiero viene en aumento. Según datos del Centro Cibernético Policial de la Policía Nacional, entre 2014 y 2016 los incidentes informáticos en contra el sector financiero aumentaron del 5,0% al 14,0% de los crímenes denunciados en el país (Gráfico R7.2). En ese último año los más afectados fueron

Gráfico R7.2
Porcentaje de incidentes informáticos en Colombia por sector



Fuente: Centro Cibernético Policial de la Policía Nacional (*Amenazas del Cibercrimen en Colombia,* 2016-2017).

1 Consultar:http://www.independent.co.uk/news/business/news/hackers-steal-2bn-rubles-from-russias-central-bank-cyber-attack-a7453991.html

2 Consultar: https://thehackernews.com/2016/05/swift-banking-hack.html

3 Consúltese:https://www.wired.com/2015/11/four-indicted-in-massive-jp-morgan-chase-hack/

4 Consúltese:https://www.bankinfosecurity.com/qnb-confirms-leak-downplays-damage-a-9082

5 Consúltese:https://www.bankinfosecurity.com/hackers-release-info-from-swiss-bank-a-7781

6 Consúltese:https://www.cyberscoop.com/hackers-break-polish-banks-government-regulator-charged-bank-security-standards/

los ciudadanos (57,0%), seguidos por el sector financiero, las empresas de la rama tecnológica (8,0%) y las firmas industriales (7,0%).

De acuerdo con lo expuesto, queda en evidencia que hoy en día la gestión del riesgo cibernético es fundamental para las instituciones financieras, con el fin de prevenir escenarios que los lleven a experimentar pérdidas significativas. Del mismo modo, y dado el carácter sistémico del cibercrimen, las agencias reguladoras deben prestar especial atención a este riesgo, con el fin de evitar episodios que puedan terminar en crisis financieras y de mitigar los efectos en caso de su materialización. Adicional a esto, existen razones teóricas para regular y supervisar este riesgo, las cuales se derivan de que el mercado puede fallar en la provisión de un nivel de seguridad cibernética socialmente óptima, debido principalmente a la presencia de asimetrías de información, incentivos desalineados, externalidades, fallas de coordinación y concentración del riesgo (FMI, 2017).

2. Enfoques para la regulación y supervisión del riesgo cibernético

La experiencia reciente indica que el riesgo cibernético es dinámico y cambiante, maleable con la evolución tecnológica y particularmente adaptable a cambios en la regulación, supervisión y al fortalecimiento de salvaguardas en su contra. Estas características hacen que la regulación y la supervisión del riesgo cibernético sean tareas especialmente complejas que requieren herramientas y marcos analíticos especiales. Con esto, en el mundo se han empezado a proponer enfoques y principios regulatorios y de supervisión que buscan enfrentar las amenazas latentes en materia de ciberseguridad.

En cuanto a la regulación, los diversos enfoques pueden agruparse en dos categorías, dependiendo del trato que se da al riesgo cibernético en relación con otros riesgos (FSB, 2017b; BIS, 2017). En primer lugar, se ha planteado un enfoque de trato "especial" al riesgo cibernético, que consiste en incorporarlo como un riesgo específico enfrentado por los actores del mercado y que debe ser objeto de una regulación independiente de otras consideraciones (como es el caso con el riesgo de crédito, de mercado, de liquidez u operativo). Desde este enfoque (llamado *targeted approach*), se plantean dos esquemas complementarios de regulación: el primero consiste en ofrecer principios y lineamientos generales que las entidades deben cumplir (como un reconocimiento de la importancia del riesgo y el establecimiento de procesos generales de salvaguarda y responsabilidad de gobierno corporativo). El segundo consiste en ofrecer prescripciones específicas de acción, tales como estrategias de defensa o procesos de respuesta a ataques. En segundo lugar, se ha planteado un enfoque de trato "subordinado" al riesgo cibernético, que consiste en incorporarlo como un aspecto del riesgo operacional, sujeto, por tanto, a un trato que estaría contenido en las reglas establecidas para este último.

En materia de supervisión, los esfuerzos se encuentran principalmente en dos frentes. El primero es la recolección de información sobre materialización del riesgo cibernético como una actividad crucial para el monitoreo por parte de las autoridades y para el aprendizaje por parte de los participantes en el mercado. El segundo frente es el diseño de estrategias de supervisión dinámicas, entendiendo que un patrón de supervisión basado en conductas específicas podría ofrecer un mapa de acción a potenciales atacantes cibernéticos (FSB, 2017b).

3. Experiencia internacional y local

Los entes reguladores de cada país han hecho algunas propuestas para incrementar el nivel de seguridad de las entidades financieras en este frente. Además, están cada vez más interesados en compartir sus desarrollos para enfrentar esta amenaza junto con los bancos centrales. Según el Banco de Inglaterra se debe tomar conciencia del problema; es decir, no se trata de evitar los ataques cibernéticos sino de concientizar a las entidades sobre estos e incentivarlas a preparar respuestas adecuadas ante los ataques (Gracie, 2015). Con esta visión el Banco de Inglaterra ha desarrollado CBEST, que es un marco de pruebas que estresa a las entidades en términos de seguridad informática y que les permite reconocer el tipo de amenazas al que pueden verse enfrentadas ante una irrupción cibernética. Este marco de pruebas cuenta con información de inteligencia de las autoridades inglesas, lo que permite que las pruebas se realicen siempre con los hallazgos más recientes.

En Canadá, el ente supervisor publicó una guía que insta a las entidades financieras a implementar estándares de seguridad que cumplan con las mejores prácticas relacionadas con la seguridad informática. Por su parte, el banco central solicita a las infraestructuras financieras con mayor importancia sistémica completar una autoevaluación de sus prácticas de seguridad que incluyan un esquema de manejo del riesgo de ataques cibernéticos. Además, son conscientes de que un ataque de este tipo puede tener un efecto contagio dentro del sistema financiero, e incluso traspasarse a otras industrias. Con esta visión se desarrolló el Centro Canadiense de Respuesta a Ciber-Incidentes (CCIRC, por sigla en inglés), el cual se encarga de recolectar información clave sobre eventos cibernéticos. Esta es utilizada por las entidades participantes para diseñar respuestas proactivas que puedan prevenir la materialización del riesgo. Además, cuentan con el Programa Conjunto de Resiliencia Operacional (JORM, por su sigla en inglés), que se encarga de proponer ejercicios en ambientes de estrés bajo los cuales las entidades pueden probar sus habilidades para incidentes (Bank of Canada, 2014).

En Latinoamérica, la Superintendencia de Bancos e Instituciones Financieras de Chile presentó una circular sobre seguridad de la información y ciberseguridad, donde exhorta a las entidades financieras a tomar decisiones con el fin de mitigar los efectos derivados de un ataque cibernético y a realizar revisiones periódicas de sus sistemas para evaluar su capacidad de respuesta ante la ocurrencia de un evento. Además, en la actualidad se está contemplando la creación de un Grupo de Trabajo de la Industria, el cual se encargaría de recopilar información sobre ataques y coordinar a las entidades para implementar las mejores prácticas junto con los entes policiales y las agencias de inteligencia.

En Colombia algunas entidades financieras ya están empezando a considerar el riesgo cibernético como una de las amenazas para su desempeño: un ciberataque se materializaría en la pérdida de confianza de sus clientes. Sin embargo, el porcentaje de entidades que considera que este riesgo podría afectarlas es bajo (1,0%; Banco de la República, 2017), si se compara con la percepción que existe en otros países como Inglaterra (51,0%; Bank of England, 2017). Por su parte, el Banco de la República ha comenzado con la concientización del riesgo, al participar en foros y mesas interinstitucionales que trabajan en torno al riesgo cibernético. Dentro del Banco se ha adoptado una estrategia de blindaje tecnológico que incluye análisis de riesgos en procesos y en la tecnología SWIFT, con colaboración del Grupo Internacional de Trabajo en Riesgo Operacional (IORWG, por su sigla en inglés). Por su parte, la SFC ha emitido algunos pronunciamientos al respecto, como la Circular Externa 052 de 2007, en la que se estipulan los requisitos mínimos de seguridad que las entidades financieras deben tener para la distribución de los productos y servicios que ofrecen a sus clientes. Además, exige que en el marco del Sistema de Administración del Riesgo Operativo (SARO) se realicen controles periódicos de recuperación ante ataques cibernéticos. Por último, esta entidad, junto con algunas vigiladas, se encuentra trabajando en la implementación del documento CONPES (2016) para la Política Nacional de Seguridad Digital.

4. Principios para mejores prácticas en regulación y supervisión del riesgo cibernético

Como resultado de la experiencia en materia de ciberseguridad, y con base en los enfoques generales presentados, es posible identificar un conjunto tentativo de principios que pueden servir de base a la determinación de mejores prácticas en regulación y supervisión del riesgo cibernético. Entre ellos se destacan los siguientes:

a. **La regulación y supervisión del riesgo deben ser prospectivos.** Si bien el esfuerzo de recolección de información es crucial para entender la forma de operación del riesgo, las amenazas cibernéticas cambiantes hacen que la experiencia pasada sea menos útil en este contexto en comparación con los riesgos tradicionales de los participantes. Un enfoque abierto y flexible que pueda responder a esta dinámica podría ser más conveniente para enfrentar el riesgo.

b. **Algunos de los viejos principios regulatorios no necesariamente aplican al riesgo cibernético.** Si bien el capital bancario contribuye a alinear los incentivos de los participantes en el mercado y a permitirle al sistema contar con mayor resiliencia ante choques, frente al riesgo cibernético no es claro que cumpla alguno de estos roles. Entidades con un alto capital bancario pueden verse seriamente afectadas por el riesgo cibernético sin que el capital contribuya a moderar los efectos de su materialización.

c. **La prescripción de conductas específicas no es deseable.** Por las razones descritas, anteriormente, un conjunto de recetas específicas impuestas por el regulador ofrecería un mapa de acción a potenciales atacantes; a diferencia de otros riesgos, la falta de transparencia sobre las estrategias específicas de control de riesgo y de respuesta no es necesariamente indeseable.

d. **La puesta a prueba de estrategias es un componente importante del enfoque de supervisión.** Al respecto, múltiples enfoques novedosos han sido experimentados, basados en el uso de ataques simulados (*red teaming*) o de recompensas a expertos en la búsqueda de falencias (*bug bounty*).

e. **Las estrategias de respuesta son potencialmente más importantes que las de defensa.** Es necesario reconocer que la velocidad a la que avanza el riesgo cibernético es mayor a la capacidad para regularlo. Si bien enfoques prospectivos y flexibles ofrecen una mejor oportunidad de prevenir ataques, es necesario reconocer la inevitabilidad de algunos de ellos. Al respecto, es importante que los participantes y las autoridades dediquen esfuerzos a afinar estrategias de respuesta una vez ha ocurrido un ataque.

f. **La cooperación internacional es fundamental.** La experiencia internacional sugiere que el crimen cibernético es usualmente transnacional y difícilmente trazable dentro de fronteras y jurisdicciones individuales. Por lo anterior, el papel de las instituciones multilaterales en materia de coordinación regulatoria, captura y distribución de información entre autoridades nacionales adquiere relevancia especial en este contexto.

Referencias

Banco de la República (2017). "Encuesta de percepción sobre riesgos del sistema financiero". Julio de 2017.

Bank for International Settlements (BIS, 2017). "Regulatory Approaches to Enhance Banks' Cyber-security Frameworks". FSI Insights on Policy Implementation, núm 2, BIS.

Bank of Canada (2014). “Cyber Security: Protecting the Resilience of Canada’s Financial System”. Financial System Review, diciembre de 2014.

Bank of England (2017). “Systemic Risk Survey”. 2017 H1.

Conpes (2016). “Conpes 3854: Política Nacional de Seguridad Digital”. Documentos Conpes, 11 de abril de 2016.

Financial Stability Board (FSB, 2017a). “Financial Stability Implications from FinTech”. Supervisory and Regulatory Issues that Merit Authorities’ Attention.

Financial Stability Board (FSB, 2017b). “Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices”.

Fondo Monetario Internacional (FMI, 2017). “Cyber Risk, Market Failures, and Financial Stability”, IMF Working Paper. Western Hemisphere and Monetary and Capital Markets Departments.

Gracie, Andrew (2015). “Cyber resilience: A Financial Stability Perspective”, Cyber Defense and Network Security Conference, Londres, 23 de enero de 2015.

Verizon (2016). “Data Breach Investigations Report 2016”, Verizon Enterprise. URL: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf