Taller 6
Ciberseguridad y resiliencia operacional

Preside: Lyndon NELSON (Deputy Chief Executive de la Autoridad de Conducta Financiera del Reino Unido y Executive Director of Regulatory Operations & Supervisory Risk Specialists del Banco de Inglaterra)

El aumento de los riesgos de ciberseguridad puede tener consecuencias para la estabilidad financiera

En marzo de 2017, los ministros de finanzas y gobernadores de bancos centrales del G-20 señalaron que «el uso malicioso de las tecnologías de la información y la comunicación (TIC) podría perturbar servicios financieros cruciales para los sistemas financieros tanto nacionales como internacionales, menoscabar la seguridad y la confianza y poner en peligro la estabilidad financiera»[1]. La rápida propagación del ransomware WannaCry y la detección de un robo de información de carácter personal que afectó a más de 140 millones de cuentas de Equifax en mayo del mismo año intensificaron la sensación de que es urgente coordinar los esfuerzos internacionales para reforzar la resiliencia a ataques cibernéticos del sistema en su conjunto.

Aunque los ciberataques a gran escala en forma de denegación de servicio distribuido, robo de datos, pérdida de propiedad intelectual y fraude cibernético existen desde hace 15 años, su frecuencia y sus efectos han aumentado a mayor velocidad que la capacidad de las empresas para evitarlos o recuperarse tras cada uno de ellos. Según un reciente informe, la ciberdelincuencia cuesta actualmente a las empresas en torno a 600 000 millones de dólares, frente a los 445 000 millones de dólares de 2014, lo que la convierte en la tercera lacra global en términos económicos, tras la corrupción en las administraciones públicas y el tráfico de drogas [2]. Aunque los problemas de ciberseguridad afectan a todos los sectores y regiones, es posible que los bancos sean el objetivo favorito de este tipo de delincuentes. En 2017, un estudio estimó que una institución financiera típica sufre un promedio de 85 ciberataques selectivos cada año, un tercio de los cuales tiene éxito[3].

Esta aceleración de la tendencia se debe tanto a la mayor velocidad del cambio tecnológico como al ecosistema cada vez más interconectado del que forman parte los bancos. Además, la banca es un sector basado en datos, por lo que los bancos compiten por clientes con otros actores de industrias basadas en datos en cada uno de los eslabones de su cadena de valor. En particular, los principales determinantes de la competencia por clientes en un entorno en el que las redes sociales proporcionan

[1] Véase G-20, *Communiqué: G20 Finance Ministers and Central Bank Governors Meeting, Baden-Baden, Germany, 17-18 March 2017*, en http://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Featured/G20/g20-communique.pdf?__blob=publicationFile&v=3.

[2] McAfee en asociación con el Center for Strategic and International Studies (CSIS), febrero de 2018 https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf.

[3] Accenture (2017). *High Performance Security Report 2016 https://www.accenture.com/us-en/insight-building-confidence-facing-cybersecurity-conundrum.*

plataformas globales instantáneas son el plazo de comercialización y la calidad de la experiencia del cliente, y existe el riesgo de que estos dos factores se optimicen en detrimento de la seguridad y la solvencia. Los bancos están adoptando estrategias de automatización e integración que les obligan a almacenar y tratar más datos fuera de sus perímetros regulados y, al mismo tiempo, a conceder a proveedores de servicios, incluidas entidades *fintech*, acceso a sus entornos para realizar procesos de negocio y tecnológicos. Esto genera una superficie de ataque accesible desde cualquier lugar e incentiva a los ciberdelincuentes a incrementar su capacidad.

A escala sistémica, el Fondo Monetario Internacional (FMI) destaca las ciberamenazas como un riesgo para la estabilidad financiera en su Informe sobre la estabilidad financiera mundial (GFSR, octubre de 2017[4]) y las autoridades nacionales han comenzado a tener en cuenta el ciberriesgo en sus informes periódicos sobre la estabilidad financiera[5]. Entre los posibles canales de transmisión identificados en dichos informes, los más citados son las interconexiones financieras, las dependencias operacionales y los efectos sobre la confianza, aunque tanto las instituciones financieras como el sector oficial tienen dificultades para encontrar un conjunto de parámetros significativos y comparables para cuantificar y vigilar el ciberriesgo y valorar los niveles de ciberresiliencia de las empresas.

P1. ¿Qué retos concretos plantea el ciberriesgo en contraposición con los riesgos operacionales tradicionales?

P2. ¿Existe alguna innovación o algún avance tecnológico concreto en el ecosistema actual que entrañe riesgos sistémicos de ciberseguridad que los supervisores deban vigilar atentamente?

Respuestas oficiales hasta la fecha

La ciberseguridad fue objeto de debate en el ICBS celebrado en noviembre de 2016, en el marco de un taller sobre «el refuerzo de las buenas prácticas para servicios bancarios». Se analizaron los riesgos que los ciberataques entrañan para el sistema financiero en su conjunto, en especial la importancia del elemento humano —desde la falta de conocimientos y competencias de los consejos de administración y del personal hasta las dificultades para reclutar y retener profesionales expertos—, más allá de los aspectos técnicos del mantenimiento del software y el hardware. Hace dos años, se esperaba que en un buen número de jurisdicciones se promulgara legislación en materia de ciberseguridad y protección del consumidor para estipular la obligatoriedad de «ciertos elementos de buen gobierno corporativo y el cumplimiento de determinados estándares tecnológicos».

Hace menos de un año, la ciberseguridad alcanzó el primer puesto de la lista de prioridades de los reguladores internacionales y desde entonces es el centro de atención de la mayoría de los organismos de normalización internacionales, no solo en el sector financiero. En paralelo, los bancos han reforzado y mejorado su capacidad para hacer frente a las nuevas amenazas emergentes. El FSB publicó en octubre de 2017 un repaso de la regulación, las directrices y las prácticas de supervisión en materia de ciberseguridad publicadas a escala tanto nacional como internacional. Dicho ejercicio permitió constatar que la banca es el único sector de servicios financieros para el que todas las jurisdicciones pertenecientes al FSB han publicado como mínimo una regulación, directriz o práctica supervisora y que tres cuartos de los encuestados (tanto jurisdicciones miembros como organismos internacionales) tenían «planes» para publicar material «en el plazo de un año». Además, las jurisdicciones miembros del FSB respondieron que

[4] Véase FMI (2017), *Informe sobre la estabilidad financiera mundial*, octubre. https://www.imf.org/es/Publications/GFSR/Issues/2017/09/27/global-financial-stability-report-october-2017.

[5] Por ejemplo, véanse los recientes informes de estabilidad financiera de Canadá, la India, Países Bajos, Sudáfrica, del Financial Stability Oversight Council y la Office of Financial Research de Estados Unidos y del BCE.

para elaborar sus marcos de regulación y supervisión de la ciberseguridad se basaban en un reducido conjunto de orientaciones o normas nacionales e internacionales de autoridades públicas u organismos privados (fundamentalmente, las directrices *Guidance on cyber resilience for financial market infrastructures* del Comité de Pagos e Infraestructuras del Mercado (CPMI) y la Organización Internacional de Comisiones de Valores (OICV-IOSCO) publicadas en junio de 2016, el marco de ciberseguridad del NIST estadounidense[6] y la serie ISO 27000). Otras iniciativas internacionales citadas por las jurisdicciones miembros incluían los *Fundamental Elements of Cybersecurity for the financial sector* del Grupo de los Siete (G-7)[7] y, en la UE, el Plan de acción en materia de tecnología financiera de la Comisión, que invita a las Autoridades Europeas de Supervisión a considerar la posibilidad de elaborar directrices para la convergencia en materia de riesgos relacionados con las TIC[8].

Por otra parte, aunque bancos y reguladores están de acuerdo en que las directrices actualmente vigentes proporcionan un conjunto sólido de principios de alto nivel que pueden servir como punto de partida para mejorar la ciberseguridad, las partes interesadas de la industria coinciden en señalar como un problema la dedicación de recursos y tiempo a ejercicios de cumplimiento burocráticos sin utilidad real, en ocasiones con regulaciones redundantes o contradictorias, en lugar de dedicarlos a reforzar y mantener de forma efectiva su capacidad de resiliencia[9]. Desde el punto de vista del sector oficial, la diversidad de marcos institucionales nacionales de ciberseguridad y los distintos grados de madurez de las iniciativas sectoriales también constituyen un reto para diseñar políticas eficaces, en un contexto en el que la fortaleza del sistema está determinada por su eslabón más débil.

P3. ¿Existen casos concretos de fragmentación regulatoria (geográfica, sectorial, etc.) en los que la acumulación de requerimientos en realidad debilita las posiciones de las instituciones? En caso afirmativo, ¿qué puede hacerse para solucionarlo?

De la ciberseguridad a la resiliencia operacional

Conforme crecía el número, la sofisticación y los efectos disruptivos de los ciberataques, también iban aumentando paulatinamente los niveles de madurez en el sistema financiero, que ha ido aprendiendo de su experiencia. A continuación se relacionan algunas de las principales lecciones en las que se basan las medidas tomadas por bancos y reguladores:

- **La gran mayoría de los ciberataques que logran su objetivo pueden clasificarse como problemas básicos de higiene cibernética**. Esto significa que las grandes inversiones en capacidades y tecnologías sofisticadas no garantizan necesariamente una protección más eficaz si la gestión de contraseñas, acceso y revisiones sigue siendo deficiente. Los responsables de los ciberataques estudian los sistemas a los que atacan y realizan pruebas para detectar posibles vulnerabilidades empezando con las funciones más básicas, a menudo con un correo electrónico de suplantación de identidad (*phishing*) enviado a un empleado. Empresas y autoridades deben garantizar de forma continua un nivel básico de seguridad, concienciación y familiaridad con

[6] NIST significa National Institute of Standards and Technology.

[7] Véase los *Fundamental Elements of Cybersecurity for the Financial Sector* del G-7, octubre de 2016.

[8] La Autoridad Europea de Valores y Mercados (AEVM), la Autoridad Bancaria Europea (ABE) y la Autoridad Europea de Seguros y Pensiones de Jubilación (AESPJ), conocidas conjuntamente como las «Autoridades Europeas de Supervisión».

[9] FSI Insights, nº 2, Regulatory approaches to enhance banks' cyber-security frameworks, agosto de 2017, disponible en https://www.bis.org/fsi/publ/insights2.pdf.

herramientas y prácticas informáticas de todo el personal, los procesos y la tecnología relevantes para las operaciones de una empresa.

- **Con los ciberincidentes, la pregunta es cuándo ocurrirán, no si ocurrirán**. Las amenazas pueden ser tanto externas como internas y, si no se detectan, los fallos o brechas de seguridad pueden seguir ocultos durante meses, lo que significa que las instituciones pueden caer en una falsa sensación de seguridad que en última instancia les haga más vulnerables. Las empresas pueden ser incluso víctimas colaterales de ataques no dirigidos inicialmente contra ellas (por ejemplo, el caso de la infección de NotPetya que afectó a Maersk), lo que significa que deben prepararse para lo inesperado y prestar atención a lo que ocurre en otros países e industrias.
- **La ciberseguridad tiene repercusiones operacionales, pero también para la actividad principal de la empresa.** La ciberseguridad ha dejado de ser un problema de las tecnologías y los sistemas de la información y la comunicación. Todas las funciones, servicios y productos operados y diseñados por empresas tienen un perfil de ciberriesgo concreto, que a su vez tiene distintos efectos sobre la actividad de la empresa. Ninguna medida de capital o liquidez puede proteger de las consecuencias de que un servicio o función esencial se vea comprometido, con la consiguiente perturbación o interrupción de actividades esenciales. Por lo tanto, la dimensión de la ciberseguridad no solo ha de formar parte de las estrategias de negocio aprobadas por el máximo órgano directivo de la empresa, sino que también debe integrarse en las actividades cotidianas para construir procesos, servicios y productos que sean seguros por su propio diseño.

Gracias a estas sencillas observaciones, actores tanto del sector privado como del público han comenzado a abordar la gestión de los ciberriesgos desde una perspectiva estratégica y de resiliencia operacional más amplia, en lugar de tratarla como una disciplina meramente técnica centrándose en la seguridad[10]. Si se adopta un punto de vista integrador, la dimensión de la ciberseguridad puede considerarse un elemento muy importante de la resiliencia operacional. Sea cual sea el nivel de protección, debemos esperar que en algún momento se produzca un incidente, por lo que el planteamiento de gestión del riesgo no solo debe garantizar que existan controles y mecanismos de mitigación, sino también prever cómo responder, recuperarse y aprender de esa brecha. Para este tipo de planificación de contingencias y continuidad es necesario que los sistemas de una empresa estén clasificados por su nivel de importancia, así como que se defina un nivel de apetito por el riesgo para los activos y negocios de la empresa por medio de parámetros pertinentes. Este tipo de planteamiento se utiliza también cuando se producen perturbaciones del funcionamiento normal cuya causa no es un ciberataque (por ejemplo, las catástrofes naturales o los fallos de un proveedor externo de servicios críticos del banco).

Trabajo del Comité de Basilea en materia de resiliencia operacional

En este contexto, el Comité de Supervisión Bancaria de Basilea (BCBS) reconoció los beneficios de abordar la resiliencia operacional más allá del ámbito de la gestión del riesgo operacional y los requerimientos de capital mínimos, y a principios de 2018 estableció el grupo de trabajo de resiliencia operacional (ORG) con la intención de contribuir, entre otras cosas, a los esfuerzos internacionales relacionados con la gestión del ciberriesgo.

El primer cometido del ORG ha sido identificar las prácticas actualmente vigentes en el ámbito de la ciberresiliencia, así como evaluar las deficiencias y las medidas de política que podrían mejorar la

[10] Por ejemplo, el Banco de Inglaterra ha publicado un documento de debate concebido para «iniciar un diálogo con la industria de servicios financieros para lograr un cambio sustancial en la resiliencia operacional de las empresas y las infraestructuras del mercado financiero». Véase *Building the UK financial sector operational resilience*, julio de 2018, disponible en https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf?la=en&hash=4238F3B14D839EBE6BEFBD6B5E5634FB95197D8A.

resiliencia operacional general de los bancos en el futuro. Con la puesta en marcha de esta iniciativa, el Comité reconocía la necesidad de que el ORG tenga debidamente en cuenta los distintos marcos internacionales y nacionales que ya existen o están en fase de desarrollo. La participación de los miembros del ORG en los correspondientes grupos de trabajo del CPMI, el FSB, las autoridades regionales y las iniciativas sobre ciberseguridad del G-7 refleja el interés del Comité por lograr una estrecha vigilancia y coordinación internacional en todo el sector financiero. En solitario, el BCBS había publicado ya en 2003 y 2011 dos documentos sobre la materia, los *Principles related to the risk management of "electronic banking"*[11] y los *Principles for the sound management of operational risk*[12]. También había publicado, conjuntamente con la OICV-IOSCO y la IAIS en el contexto del Foro Conjunto, unas directrices para la externalización de servicios financieros en 2005[13] y unos principios de alto nivel sobre continuidad del negocio en 2006[14]. Partes de estas directrices y principios de alto nivel continúan siendo válidas y deberían sentar los cimientos para el futuro trabajo de política, mientras que otras partes que están desactualizadas o son redundantes podrían simplificarse. En términos generales, la mayor parte de las iniciativas internacionales pasadas y actuales tratan los temas que se relacionan a continuación, que engloban las principales preocupaciones de los supervisores en materia de resiliencia operacional:

- marcos de gobernanza, incluidas las funciones del consejo de administración y el director de seguridad de la información;
- análisis y valoración del ciberriesgo;
- seguridad de la información, incluida la confidencialidad;
- controles de seguridad y prevención de incidentes;
- conocimientos especializados, formación y mayor sensibilización cultural para gestionar y atajar riesgos;
- vigilancia, pruebas y/o auditoría de controles, incluso mediante la creación de equipos rojos o morados;
- respuesta y recuperación de incidentes para investigar, gestionar y contener incidentes, y recuperarse tras ellos;
- comunicación e intercambio de información con partes interesadas internas y externas, públicas y privadas, a escala intersectorial y transfronteriza;
- relaciones de externalización y dependencia de terceros en general: el perímetro de interés para los reguladores del sector financiero se ha ampliado, y el mayor uso de servicios de computación en la nube significa que dicho perímetro también está compartido; y
- aprendizaje continuo para reevaluar, someter a pruebas y mejorar la resiliencia de forma continua, también mediante ejercicios y la cooperación entre las esferas pública y privada.

En lo que respecta a la evaluación de las distintas prácticas actuales, los supervisores intercambian experiencias directas y observaciones con el fin de conocer mejor las principales tendencias, los avances realizados y las deficiencias en la búsqueda de la ciberresiliencia en el sector bancario. El BCBS también se ha comprometido a mantener un diálogo permanente con una amplia variedad de partes interesadas,

[11] Comité de Supervisión Bancaria de Basilea. *Risk Management Principles for Electronic Banking*, julio de 2003, disponible en www.bis.org/publ/bcbs98.pdf.

[12] Comité de Supervisión Bancaria de Basilea. *Principles for the Sound Management of Operational Risk*, junio de 2011, disponible en www.bis.org/publ/bcbs195.pdf.

[13] Foro Conjunto, febrero de 2005, disponible en https://www.bis.org/publ/joint12.pdf.

[14] Foro Conjunto, agosto de 2006, disponible en https://www.bis.org/publ/joint17.pdf.

incluso de fuera de la industria bancaria, para incorporar sus sugerencias a la labor que viene realizando para diseñar posibles medidas de política destinadas a mejorar la resiliencia operacional general de los bancos en los próximos años.

P4. ¿Qué parámetros o indicadores podrían utilizar los bancos para evaluar y comparar los niveles de resiliencia operacional de sus proveedores de servicios externos, y los supervisores a la hora de evaluar y comparar la resiliencia de los bancos?

P5. ¿Qué prácticas han resultado eficaces para desarrollar e implementar un marco de resiliencia operacional eficaz? ¿Cuáles son las prácticas emergentes en este ámbito?

P6. ¿Cómo puede mejorarse el intercambio intersectorial y transfronterizo de información entre bancos y reguladores?

P7. ¿Cuál podría ser la mejor forma de solucionar las dificultades que afrontan las instituciones a la hora de desarrollar sus competencias y capacidades cibernéticas?

P8. ¿Qué dificultades prácticas plantea la interacción con proveedores de servicios externos? ¿Qué dificultades encuentran los proveedores externos para cumplir los requisitos bancarios actualmente vigentes?

P9. ¿Hay problemas de implementación relacionados con diferencias estructurales o regionales que merecerían un examen más exhaustivo por parte del Comité de Basilea? ¿Dónde reportaría mayores beneficios la normalización?