Temático

CIBERRIESGOS

El ciberriesgo se puede definir como la combinación de la probabilidad de ocurrencia de ciberincidentes, esto es, eventos que comprometan la confidencialidad, la integridad o la disponibilidad de la información y/o los sistemas de información, sean producto de actividad maliciosa o no, con su impacto[1]. Estos eventos son cada vez más relevantes para el conjunto del sistema financiero y para otros sectores productivos, debido al avance en el proceso de digitalización de la economía y la sociedad[2]. Además, debido a las interconexiones financieras y tecnológicas, los ciberincidentes pueden propagarse rápidamente entre bancos, entidades no bancarias e infraestructuras del mercado financiero, con potenciales implicaciones para la estabilidad financiera. La dependencia de servicios críticos proporcionados por terceros supone nuevas vulnerabilidades y riesgos de concentración dentro del sistema financiero.

En este contexto, los reguladores y supervisores prudenciales están prestando una atención prioritaria a estos riesgos e impulsando distintas iniciativas para aumentar la resiliencia de las entidades financieras frente a los mismos, esto es, para reforzar su ciberresiliencia. La iniciativa de las autoridades refuerza los incentivos, ya de por sí, elevados de las entidades financieras para invertir en recursos tecnológicos, no sólo para proteger sus datos, sino también la integridad de la provisión de servicios a sus clientes.

Entre las iniciativas de las autoridades europeas destacan la aprobación reciente del Reglamento DORA *(Digital Operational Resilience Act,* por sus siglas en inglés)[3], la Directiva NIS2 sobre ciberseguridad[4], los trabajos en curso para responder a la recomendación de la Junta Europea de Riesgo Sistémico (JERS) sobre la coordinación en caso de ciberincidentes sistémicos y las pruebas de resistencia con fines de supervisión de la resiliencia de los bancos frente a los ciberataques por parte del Mecanismo Único de Supervisión en 2024.

El resto del capítulo se organiza de la siguiente forma. El epígrafe T1 analiza los conceptos de ciberriesgo y de ciberresiliencia en el contexto de digitalización del sistema financiero. El epígrafe T2 describe la frecuencia e impacto creciente de los ciberriesgos. Ambas secciones recogen datos públicos sobre los ciberriesgos, sujetos a múltiples limitaciones. El epígrafe T3 recoge las distintas iniciativas de las propias entidades financieras y de las autoridades micro- y macroprudenciales, y

1 Véase el *Cyber-Lexicon* del *Financial Stability Board* (FSB, por sus siglas en inglés) para una definición de terminología de relevancia para los ciberriesgos.

2 Véase el Informe de la Comisión Europea del 24 de enero de 2024.

3 Véase el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011.

4 Directiva UE 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

de otros ámbitos, para reforzar la ciberresiliencia. El epígrafe T4 concluye con posibles perspectivas de evolución de los ciberriesgos, por ejemplo, en relación con el efecto del desarrollo de la inteligencia artificial, y de las herramientas de las entidades y las autoridades para contenerlos, que tendrán que poner el énfasis en la disposición de los recursos tecnológicos adecuados, además de los recursos financieros utilizados para absorber pérdidas operacionales.

T.1 Los ciberriesgos y el sistema financiero

T.1.1 El sistema financiero como ecosistema

El sistema financiero constituye un sistema muy complejo, formado por numerosos participantes intensamente interconectados y dependientes entre sí. Este sistema incluye las infraestructuras de mercado, los distintos tipos de entidades financieras (bancarias y no bancarias) y sus principales proveedores de servicios tecnológicos, y el conjunto de las autoridades supervisoras de todos ellos. Las entidades financieras presentan tanto interconexiones directas a través de sus activos y pasivos, como indirectas, al invertir o financiarse con el mismo tipo de instrumentos (véase el epígrafe 2 del capítulo 2 de este IEF). Adicionalmente, existen numerosas interconexiones operativas entre los participantes del sector, a través de las infraestructuras de mercado, los proveedores de servicios comunes e incluso la prestación de servicios entre entidades financieras.

Estas interconexiones entre entidades y otras características del sistema financiero hacen que el impacto de los ciberriesgos pueda llegar a poner en peligro la estabilidad financiera[5]. La materialización de ciberincidentes puede así afectar no solamente a cada participante individual, sino también extenderse y amplificarse con implicaciones sistémicas para el conjunto del sector. Además de las interconexiones, otras características relevantes del sistema financiero para valorar los ciberriesgos incluyen su fuerte dependencia de la tecnología, su atractivo para atacantes con distintas motivaciones (por ejemplo, económicas y políticas) y una gran sensibilidad a la pérdida de la confianza de sus participantes[6].

Las entidades financieras complementan sus capacidades tecnológicas mediante distintas relaciones con otros agentes. Estas incluyen la contratación de servicios de proveedores, la participación en consorcios, inversiones en *start-ups* o adquisiciones de productos de terceros.

En muchos casos, la oferta de servicios tecnológicos está fuertemente concentrada en un número relativamente pequeño de proveedores, en particular en el caso de los relacionados con la computación en la nube[7]. De hecho, algunos de estos proveedores

5 F. J. Herrera Luque, J. Munera López y P. Williams (2021), "Cyber risk as a threat to financial stability". Revista de Estabilidad Financiera - Banco de España, 40.

6 Véase el informe de la JERS *Systemic cyber risk*, de febrero de 2020.

7 La Autoridad Bancaria Europea (EBA, por sus siglas en inglés) define la computación en la nube como un modelo que permite el acceso de red ubicuo, conveniente y bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden suministrar y desplegar rápidamente, requiriendo un esfuerzo mínimo de gestión o una interacción muy limitada con el proveedor del servicio.

han pasado a ser elementos vertebradores para el sistema financiero, a un nivel comparable al de las infraestructuras de mercado. Por ejemplo, en el segmento de computación en la nube, tres empresas representan más del 60% de cuota de mercado[8] y su fallo simultáneo podría tener consecuencias operativas adversas a nivel sistémico. Constituyen, por tanto, puntos únicos de fallo, dado que los incidentes que les afectan, incluso los no intencionados, tienen impacto en el conjunto del sector. Más aún, muchos de estos proveedores prestan sus servicios también a compañías de otros sectores, pudiendo llegar a ser críticos para la economía de un país en su conjunto o incluso de un grupo de países.

Identificar todas las interdependencias existentes en el sector es un reto complejo. Las entidades financieras tradicionales se conectan entre ellas y a las infraestructuras de mercado, existen nuevos actores que ofrecen servicios financieros (por ejemplo, *fintech)*[9] y hay una creciente dependencia de los proveedores tecnológicos directos. Pero, además, existen otras dependencias de terceros no debidamente identificadas, producidas por las subcontrataciones sucesivas a lo largo de las cadenas de contratación de productos y servicios tecnológicos, sobre las que las entidades financieras tienen escaso o ningún control. Esto ha llevado a que iniciativas como el *toolkit* del FSB[10] sobre gestión de riesgos de terceros o el Reglamento DORA de la Unión Europea (UE), analizado en más detalle en el epígrafe T3, hayan puesto el foco en estas dependencias.

T.1.2 Transformación digital y exposición al ciberriesgo

El sistema financiero está fuertemente digitalizado y las entidades financieras dependen de su tecnología no solo para desarrollar el negocio, sino como un factor diferencial y competitivo. En los últimos años, el proceso de transformación digital se ha acelerado extraordinariamente[11], tanto para mejorar la eficiencia de los procesos internos de las entidades financieras como para ofrecer a sus clientes servicios flexibles, personalizados y accesibles de forma inmediata, desde cualquier lugar y con distintos tipos de dispositivos[12]. Este fenómeno se ha visto reforzado por la aparición de nuevos competidores para las entidades financieras

8 Ting Yang Koh and Jermy Prenio (2023). *Managing cloud risk – some considerations for the oversight of critical cloud service providers in the financial sector.* FSI Insights on policy implementation No 53.

9 El FSB define fintech como «innovación financiera facilitada por la tecnología que podría resultar en nuevos modelos de negocio, aplicaciones, procesos o productos con un efecto material asociado sobre los mercados financieros y las instituciones, y la provisión de servicios financieros». Las empresas que hacen uso de estas innovaciones tecnológicas son comúnmente designadas también por el mismo término.

10 Véase el informe del FSB *Enhancing third-party risk management and oversight – a toolkit for financial institutions and financial authorities,* del 4 de diciembre de 2023.

11 Según el informe del Observatorio de la Digitalización Financiera FUNCAS – KPMG La digitalización como eje de transformación bancaria, la penetración de la banca digital en España pasó del 54,9 % en 2019 al 69,6 % en 2022, superando en casi 10 puntos porcentuales la media europea de 2022 de 59,7 %. Asimismo, el informe destaca que el avance en la transformación digital fue una prioridad estratégica en 2022 para el 58 % de las entidades, por delante de la mitigación de los efectos de la inflación que fue prioridad para el 53 %.

12 Véase José Ramón Martínez Resano. (2022). *Regulating for Competition with Bigtechs: Banking-As-A-Service and 'Beyond Banking'*.

tradicionales, como son las *bigtech*[13] o las *fintech,* que pueden ofrecer soluciones muy atractivas de forma muy ágil e innovadora.

El elevado nivel de digitalización del sistema financiero incrementa su exposición al ciberriesgo. La mayor parte de las entidades financieras tienen entornos tecnológicos extraordinariamente complejos, donde conviven aplicaciones antiguas con otras que se apoyan en tecnologías más innovadoras, fruto no solo de los procesos de transformación, sino también, en algunos casos, de sucesivas fusiones y adquisiciones[14]. Esta complejidad supone un reto para las entidades a la hora de mantener un entorno de control adecuado y, por tanto, las hace más vulnerables, tanto a fallos en los sistemas como a ciberataques.

En este contexto, la pandemia del COVID-19 ha actuado como un acelerador, introduciendo cambios en el funcionamiento de las entidades financieras y en su relación con los clientes. Por ejemplo, el teletrabajo, que se mantiene estable en niveles superiores a los previos a la pandemia, ha traído consigo riesgos adicionales para las entidades y sus empleados, entre los que podemos citar los originados por los accesos a sistemas corporativos desde dispositivos personales y redes domésticas, y el manejo de datos confidenciales en los domicilios de los empleados. El acceso electrónico de los clientes a distintos servicios financieros se vio impulsado como consecuencia de las restricciones a la movilidad durante las fases iniciales de la pandemia, y parte de este impulso se ha conservado en el período posterior de normalización de relaciones sociales.

La ampliación de la oferta de servicios financieros a distancia ha aumentado la exposición de los clientes que los utilizan a ciberataques y fraudes. Se han observado crecimientos muy significativos en los casos de fraudes que utilizan ingeniería social, como el *phishing*[15]*,* el *smishing*[16]*, y* el *vishing*[17], acompañados de suplantación de sitios web y aplicaciones móviles, entre otros. A pesar de los esfuerzos de las entidades para mejorar la educación en ciberseguridad de sus clientes, algunos continúan siendo altamente vulnerables, especialmente aquellos que antes de la pandemia no hacían uso de los canales digitales.

Aunque algunos estudios sugieren que el financiero es uno de los sectores críticos mejor preparados frente a los ciberriesgos, existe una cierta heterogeneidad a nivel de entidades individuales. Si bien la mejor posición relativa del sector se debe en parte a su elevado grado de regulación y supervisión, en algunos casos las medidas de seguridad y los controles implementados por las entidades, especialmente en el caso de las más pequeñas, deben todavía mejorarse para gestionar adecuadamente los ciberriesgos.

---

13 El FSB define bigtech como «grandes compañías tecnológicas con amplias redes de clientes establecidas».

14 Véase "Evolución de los principales grupos bancarios españoles (2009-2021)", del Banco de España.

15 Los ataques de *phishing* son aquellos en los que un atacante trata de conseguir información confidencial (contraseñas, datos bancarios, etc.) de usuarios legítimos de forma fraudulenta, recurriendo a la suplantación de la identidad digital de una entidad de confianza.

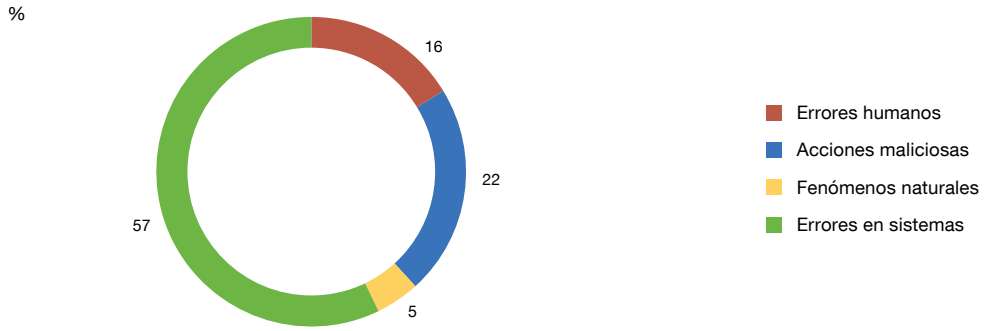
16 El *smishing* es una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima con el objetivo de robarle información privada o realizarle un cargo económico.

17 El *vishing* es un tipo de estafa de ingeniería social por teléfono; a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima.

Gráfico T.1

Pese a ser responsables de los mayores impactos, los ciberincidentes con origen malicioso representan un porcentaje reducido del total de ciberincidentes reportados

T.1.a Causas de los ciberincidentes reportados a ENISA en Europa entre 2013 y 2023



FUENTES: ENISA, *Cybersecurity Incident Reporting and Analysis System.*

T.1.3 Eventos no maliciosos y ciberataques

El concepto de ciberincidente va más allá de los ciberataques. Conviene destacar que la propia definición de ciberincidente del *Cyber Lexicon* del FSB (véase nota al pie 1) remite tanto a los de naturaleza maliciosa, causados por ciberataques, como a los no maliciosos. Estos últimos, que incluyen eventos provocados por desastres naturales (por ejemplo, terremotos), errores humanos o fallos accidentales en los sistemas, también pueden afectar a la capacidad de las entidades y del sector en su conjunto para seguir operando con normalidad, por lo que la resiliencia frente a estos ciberincidentes es igualmente relevante.

Es importante destacar las diferencias en términos de la frecuencia e impacto de los distintos tipos de ciberincidentes. Analizando las principales causas de los ciberincidentes de todos los sectores que se reportan anualmente a la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés), se observa que los no maliciosos, como fallos en los sistemas o errores humanos, son los más comunes[18] (véase gráfico T.1). A pesar de su prevalencia, estos incidentes no tienen, en la mayoría de las ocasiones, un impacto relevante ni a nivel individual ni a nivel sistémico. Son los ciberincidentes maliciosos, que representan en torno al 22 % del total, los que tienen un mayor impacto.

La propia naturaleza de los ciberincidentes maliciosos y su intencionalidad explican su mayor impacto a pesar de su menor frecuencia. En la mayoría de los casos se trata de ataques diseñados para causar el mayor impacto posible en sus víctimas; por ejemplo,

18 En este gráfico y en el resto incluidos en el capítulo temático, se ha utilizado la mejor aproximación basada en información pública para ilustrar distintos hechos estilizados relevantes relacionados con los ciberriesgos. Estas aproximaciones afrontan importantes limitaciones en cuanto a la cantidad y calidad de datos disponibles. Los supervisores disponen de datos confidenciales muy superiores. La elevada prioridad del ciberriesgo en la agenda regulatoria y supervisora hace esperar una mayor disponibilidad futura de datos agregados publicables.

paralizando sus operaciones o robando datos confidenciales. A esto hay que sumar la posibilidad de aumentar el alcance y el impacto que, en algunos casos, tienen los atacantes: de un único usuario a un grupo más amplio de una o más entidades. También contribuyen al mayor impacto los efectos a largo plazo de este tipo de incidentes, como el daño reputacional.

T.1.4 De la ciberseguridad a la ciberresiliencia

El concepto de ciberseguridad tiene un alcance bien delimitado. El *Cyber Lexicon* del FSB define la ciberseguridad como la preservación de la confidencialidad, integridad y disponibilidad de la información y/o los sistemas de información en un medio interconectado. Estamos, por tanto, ante un concepto fundamentalmente preventivo y de protección. Sin embargo, la evolución hacia un mundo completamente digital en el que las ciberamenazas son cada vez más frecuentes y sofisticadas hace necesario un cambio de paradigma, asumiendo como hipótesis de trabajo que en algún momento se producirá un ciberincidente con impacto.

El concepto de ciberresiliencia surge como evolución del concepto de ciberseguridad. El *Cyber Lexicon* del FSB define la ciberresiliencia como la capacidad de una organización para continuar llevando a cabo su misión, anticipándose y adaptándose a las ciberamenazas y a otros cambios relevantes en su entorno, resistiendo, conteniendo y recuperándose rápidamente ante ciberincidentes.

A su vez, la ciberresiliencia se puede generalizar como resiliencia operacional u operativa. El Comité de Supervisión Bancaria de Basilea (BCBS, por sus siglas en inglés), en sus *Principles for Operational Resilience*[19], definió la resiliencia operacional como la capacidad de un banco para mantener sus operaciones críticas en situaciones adversas, definición que podría aplicarse no solo a bancos, sino también a todo tipo de compañías privadas e instituciones públicas dentro y fuera del sistema financiero. Este es un enfoque más holístico, que no se centra exclusivamente en gestionar la tecnología, sino que concede la misma importancia a las personas y a los procesos de las organizaciones y enlaza con disciplinas ya existentes, como la continuidad de negocio.

T.1.5 La relación entre el ciberriesgo y los riesgos económico-financieros

Nivel individual

Los eventos de ciberriesgo pueden tener un impacto individual significativo en el ámbito operativo, pero también más allá de este. En un entorno fuertemente digitalizado, la tecnología se convierte en un factor transversal a toda la actividad del negocio, por lo que

19 Véase el informe del BCBS Principles for Operational Resilience de marzo de 2021.

el ciberriesgo puede tener impacto en otros riesgos, como el legal, el reputacional o los riesgos financieros clásicos.

Los ciberincidentes pueden llegar a generar un impacto importante sobre la reputación de una entidad. La indisponibilidad de los servicios o las vulneraciones de la confidencialidad o la integridad de la información en poder de las entidades financieras pueden tener un impacto en la confianza de los clientes y del mercado en general, tanto si son eventos maliciosos como si son accidentales. Estos impactos reputacionales pueden verse agravados si no hay una gestión adecuada de la comunicación pública cuando se producen los ciberincidentes.

Nivel sistémico

La interacción entre el ciberriesgo y otros riesgos como el financiero, no hace sino incrementarse a nivel sistémico. A las implicaciones del ciberriesgo a nivel individual se le añaden, a nivel sistémico, las derivadas del elevado nivel de interconexión e interdependencia entre las entidades financieras. Esto hace que el impacto de un ciberincidente en una entidad pueda extenderse a más entidades, agregándose el impacto operacional, financiero y reputacional y erosionando potencialmente la confianza en el sector, elemento crucial que podría incrementar exponencialmente el impacto a nivel sistémico. Otros escenarios con un potencial efecto sistémico serían, por ejemplo, un ataque masivo contra un número elevado de entidades o contra un proveedor crítico o fallos en un *software* de uso común en el sector.

Las implicaciones sistémicas para la estabilidad financiera del ciberriesgo están siendo estudiadas por las autoridades macroprudenciales. En este sentido, la JERS ha trabajado los últimos años en estudiar el impacto en la estabilidad financiera del ciberriesgo[20], los posibles canales de contagio a través de los que el impacto de un ciberincidente puede llegar a poner en riesgo la estabilidad financiera[21] y potenciales medidas para mitigarlo[22].

La materialización de riesgos vinculados al ciclo de crédito o al de negocio no reduciría necesariamente la probabilidad de ciberincidentes. Al contrario, un entorno recesivo podría incrementar los incentivos para realizar ataques maliciosos con motivación económica, ante la menor capacidad de generación de rentas legales de agentes tecnológicos o ante la reducción de la capacidad de las entidades de invertir en ciberresiliencia. Si bien es necesaria más investigación sobre esta cuestión, una relación neutra o de refuerzo de los ciberriesgos con respecto a los ciclos económico-financieros señala la necesidad de contar con recursos específicos de absorción de riesgos frente a estos. Estos recursos necesitarían su propia categoría y estarían adaptados a la naturaleza tecnológica de estos riesgos.

---

20 Véase el informe de la JERS *Systemic cyber risk* del 19 de febrero de 2020.

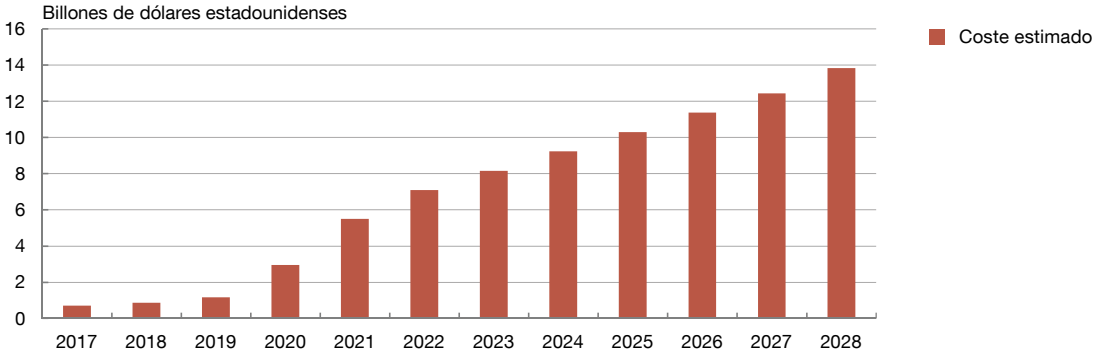
21 JERS. (2020). "The making of a cyber crash". ESRB Occasional Paper Series, 16.

22 Véase el informe de la JERS *Mitigating systemic cyber risk*, del 27 de enero de 2022.

Gráfico T.2

El coste estimado del cibercrimen a nivel mundial se ha incrementado cerca de un orden de magnitud en los últimos cinco años y se espera que esta tendencia creciente se mantenga

T.2.a Estimación del coste del cibercrimen a escala mundial



FUENTE: Statista; *Statista Technology Market Insights.*

T.2 El impacto del ciberriesgo

T.2.1 Principales ciberamenazas

Existen diferentes tipos de actores de ciberamenazas, que varían en sus motivaciones, la sofisticación de los ataques y el impacto que generan. Los atacantes aficionados[23] y los activistas[24] normalmente buscan notoriedad y suelen realizar ataques menos sofisticados y de impacto bajo o moderado. En cuanto a los denominados *insiders*[25], suelen tener como motivación la venganza o el espionaje por cuenta de otros; su conocimiento de la compañía y su facilidad de acceso los hace potencialmente peligrosos, aunque no siempre cuentan con capacidades técnicas elevadas. Sin embargo, existen otros tipos de atacantes con capacidades técnicas muy sofisticadas y capaces de producir impactos muy importantes, con motivaciones estrictamente económicas o geopolíticas.

Los ciberataques atribuidos al crimen organizado, que persiguen un beneficio económico, no cesan de incrementarse en todo el mundo. Esto está suponiendo un coste creciente (véase gráfico T.2). La legislación existente está mayormente confinada a un entorno físico y con soberanías territoriales bien definidas, lo que la hace de difícil aplicación al mundo digital. Existen, además, enormes diferencias entre jurisdicciones y los acuerdos globales para perseguir este tipo de crimen son prácticamente inexistentes. Esta situación, unida a la dificultad de la atribución de los delitos a sus responsables, convierten los ciberataques en un delito con escaso riesgo para el criminal y que supone un elevado coste para las entidades y los individuos afectados.

23 También llamados *script kiddies.*

24 Se suelen denominar *hacktivistas.*

25 En este contexto, un insider es un empleado que actúa con fines maliciosos contra su compañía.

Se ha observado también un incremento de los ciberataques con motivaciones geopolíticas. Los objetivos y las técnicas utilizadas varían de unos a otros. Así, por ejemplo, como consecuencia del conflicto entre Rusia y Ucrania, partidarios de ambos bandos han lanzado numerosos ataques de denegación de servicio[26] contra administraciones públicas y compañías de los países que apoyaban al bando contrario, para generar inestabilidad y dificultar todo tipo de actividad en ellos, incluida la financiera. Otras veces se trata de grupos respaldados por Estados que buscan monetizar sus ataques[27] mediante la realización de transferencias fraudulentas[28], el robo de criptodivisas[29] o la obtención de un rescate a cambio de devolver a sus víctimas la información cifrada por los atacantes y no divulgarla *(ransomware)*[30]. Otra vía utilizada por los atacantes para conseguir financiación es el robo de datos, y cada vez son más frecuentes los ciberataques financiados por Estados dirigidos a la obtención de información sensible que pueda ser de utilidad económica o política.

Han crecido el número y la sofisticación de los ciberataques contra proveedores del sistema financiero, realizados por los atacantes con mayores capacidades técnicas. Algunos ataques se limitan a explotar vulnerabilidades existentes en los productos de *hardware* o *software* de estos proveedores[31]. Otros, más sofisticados, alteran dichos productos para introducirles debilidades que luego puedan ser explotadas[32]. A pesar del tiempo y de los recursos necesarios para preparar y ejecutar una operación de estas características, los atacantes pueden conseguir llegar a miles de organizaciones y empresas a través de un único punto de entrada, multiplicando extraordinariamente la eficacia y eficiencia de su ataque.

T.2.2 Ciberincidentes y pérdidas

Volúmenes de ciberincidentes

En términos globales, el número de ciberincidentes no ha parado de crecer en los últimos años, con un repunte especialmente relevante de los de naturaleza maliciosa tras la pandemia de COVID-19. Como cabría esperar, el incremento de la digitalización tanto en empresas como en particulares y organismos públicos ha supuesto un aumento

26 Un ataque de denegación de servicio consiste en inundar de peticiones un sitio web hasta dejarlo inoperativo.

27 Informe del Consejo de Seguridad de las Naciones Unidas (2019).

28 Por ejemplo, el ataque al Bangladesh Bank (banco central de Bangladés) en 2016, en el que se realizaron transferencias fraudulentas a través de SWIFT por valor de más de 80 millones de dólares. Véase noticia de prensa.

29 Por ejemplo, se estima que el grupo Lazarus, asociado al Gobierno de Corea del Norte, fue responsable del 20 % de los robos de criptoactivos durante 2023, más de 300 millones de dólares. Véase noticia de prensa.

30 Un *ransomware* es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción. En numerosas ocasiones dicho rescate consiste en una cantidad de criptomonedas.

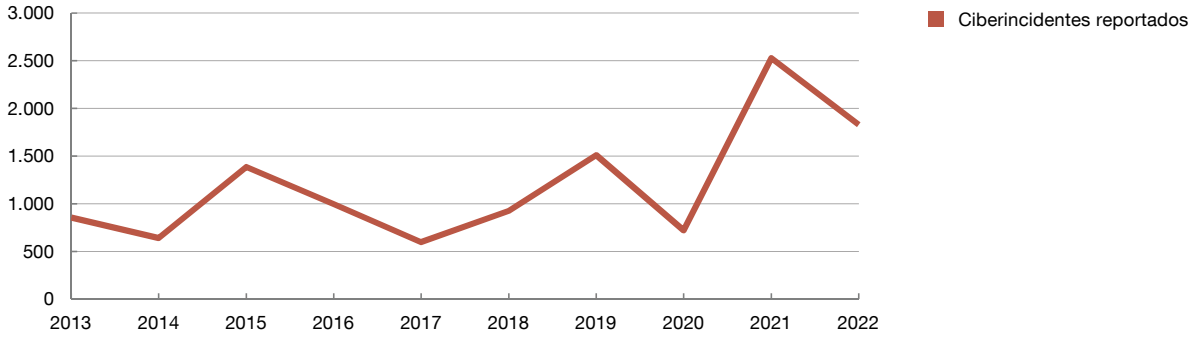
31 Hay numerosos ejemplos, se puede citar la explotación de una vulnerabilidad en el software comercial de transferencia de ficheros MOVEit por parte del grupo de ransomware ClOp, que afectó a miles de organizaciones en todo el mundo en 2023. Véase noticia de prensa.

32 El caso paradigmático es el de SolarWinds. En diciembre de 2020 se descubrió que un software distribuido por la compañía había sido alterado por un grupo de ciberatacantes para que les permitiera acceso a todos los clientes que usaban este producto. Entre los miles de afectados se encontraban numerosas agencias federales estadounidenses, así como la OTAN, el Parlamento Europeo, compañías como Microsoft, y otras. Véase noticia de prensa.

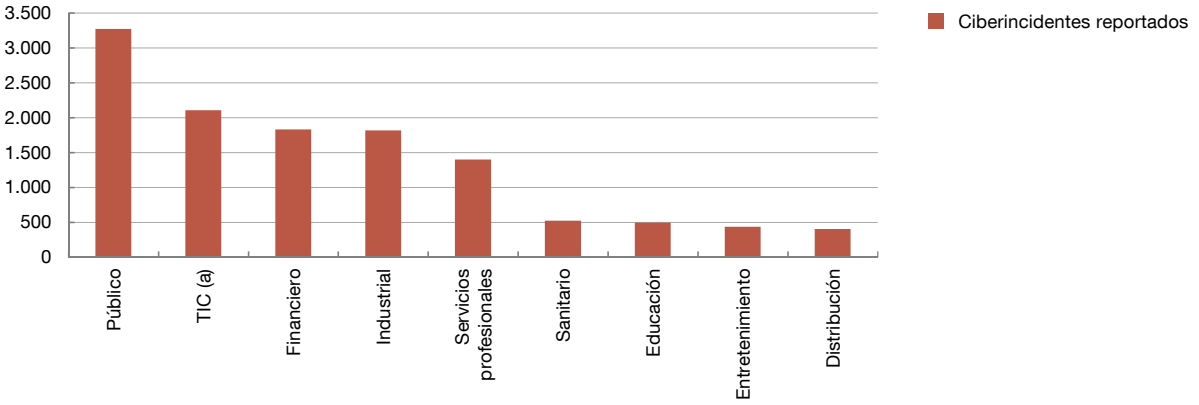
Gráfico T.3

El sector financiero continúa siendo, a escala global, uno de los que más ciberincidentes tiene. El número anual de ciberincidentes reportado en el sector financiero sigue una tendencia creciente, habiendo visto duplicado su número entre 2018 y 2022

T.3.a Número global de ciberincidentes en el sector financiero



T.3.b Número global de ciberincidentes en 2022 por sector



FUENTE: Verizon, *Data Breach Investigations Report 2023*.

a Tecnologías de la información y de la comunicación.

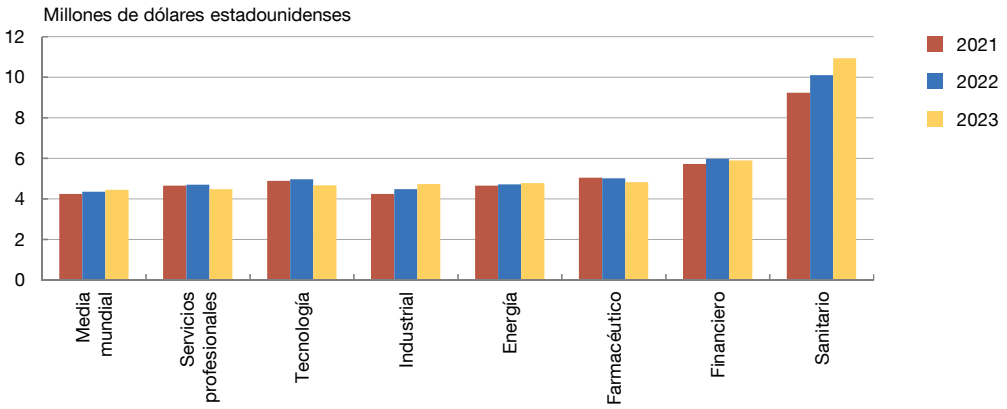
continuado de los ciberincidentes. Por ejemplo, se puede observar que el abrupto incremento del uso de la tecnología en el contexto de la irrupción de la pandemia de COVID-19 generó un significativo aumento global en el número de ciberincidentes reportados en el sistema financiero (véase gráfico T.3.a). Si bien tras el pico de la pandemia el aumento se ha moderado, cabe esperar que la tendencia siga siendo ascendente en el futuro.

El sistema financiero se sitúa entre los más atacados. Esta elevada prevalencia relativa de ciberincidentes en el sistema financiero (véase gráfico T.3.b) se mantiene a pesar de que, puntualmente, otros sectores puedan acaparar los ataques. Por ejemplo, el sector sanitario se situó entre los más atacados durante la pandemia de COVID-19 y en 2022 las administraciones públicas fueron el principal objetivo, en un contexto de tensiones geopolíticas (véase gráfico T.3.b).

Gráfico T.4

El coste medio para el sector financiero de los ciberincidentes con filtración de datos es el segundo más alto a escala global, solo superado por el sector sanitario

T.4.a Coste medio de un ciberincidente con filtración de datos por sector



FUENTES: IBM, Ponemon Institute, *Cost of Data Breach Report 2023*.

Pérdidas

Las pérdidas asociadas a un ciberincidente pueden variar considerablemente en función de distintos factores. Como se ha visto anteriormente, por su potencial para generar un mayor impacto, los ciberincidentes maliciosos normalmente llevan asociado un mayor volumen de pérdidas para la entidad. Las filtraciones de información son uno de los ciberataques más frecuentes y con más perdidas asociadas para una entidad. El coste medio de este tipo de incidentes para las entidades aumenta cada año, situándose en 4,45 millones de dólares en 2023 a escala global[33]. El sistema financiero, además de ser de los más atacados, se encuentra entre los que mayor coste medio soporta para los ciberincidentes de filtración de datos, 5,9 millones de dólares en 2023 (véase gráfico T.4).

Los ciberseguros como mitigante parcial

La transferencia del riesgo es una estrategia con alcance limitado en el caso del ciberriesgo. Las pólizas para cubrir el ciberriesgo, también conocidas como «ciberseguros», tienen un efecto limitado, ya que las coberturas financieras que ofrecen pueden no ser suficientes para mitigar el impacto de un ciberincidente. Por ejemplo, el cobro de una indemnización no puede cubrir algunos de los impactos más importantes de un *ransomware*, como es la parada de los sistemas infectados de una entidad, que debe ser resuelta con la mayor rapidez posible.

33 Véase el informe de IBM *Cost of a Data Breach Report 2023*.

Adicionalmente, se han endurecido las condiciones para los ciberseguros a escala global. El sector asegurador comenzó a cubrir el ciberriesgo sin información histórica ni conocimiento suficiente para estimar correctamente las primas. A esto se le sumó el gran incremento de la frecuencia e impacto de los ciberincidentes, lo que trajo consigo un aumento de los siniestros de ciberseguros comunicados; por ejemplo, cuadruplicándose en España entre 2017 y 2020[34]. Este incremento, sumado a unas primas bajas, tuvo un impacto negativo en la rentabilidad de este tipo de seguros. Las compañías aseguradoras han reaccionado en los últimos años endureciendo las condiciones de renovación, incrementando las primas o añadiendo clausulado especial para excepcionar de las coberturas circunstancias como *ransomware* o guerras.

T.3 Gestionar el ciberriesgo para alcanzar la resiliencia individual y sistémica

T.3.1 Buenas prácticas, regulación y supervisión

La discusión sobre el ciberriesgo en el sistema financiero ocupa un lugar relevante en la agenda de numerosos organismos internacionales. En paralelo al incremento de la digitalización de toda la actividad económica y del consecuente aumento de la exposición al ciberriesgo, estos organismos internacionales han emitido buenas prácticas, informes y herramientas. Entre los trabajos más relevantes de los últimos años para el sistema financiero, el FSB publicó la mencionada taxonomía *Cyber Lexicon,* así como unas prácticas efectivas para la respuesta y recuperación ante ciberincidentes[35], y está actualmente trabajando en un formato común para su notificación[36].

En este ámbito destaca la emisión por parte del Comité de Supervisión Bancaria de Basilea de los Principios de Resiliencia Operacional[37]. Estos tienen el propósito de reforzar la capacidad de los bancos de resistir el impacto de eventos operacionales que pueden causar disrupciones de sus servicios críticos. El Comité señala que los bancos deben asumir como hipótesis de trabajo que este tipo de eventos ocurrirán y definir su nivel de tolerancia a la disrupción. Los principios abarcan tanto medidas preventivas y de anticipación como otras encaminadas a la respuesta y recuperación cuando se produce la disrupción en servicios críticos. Estos principios cubren aspectos de i) gobernanza, ii) gestión de riesgos operacionales e identificación continua de amenazas, iii) identificación de interconexiones e interdependencias, iv) gestión de terceras partes, v) continuidad de negocio, vi) gestión de incidentes y vii) gestión de la tecnología, incluida la ciberseguridad. Desde su publicación, las jurisdicciones han trabajado para incorporar estos principios a su marco

34 Según el IV Estudio Anual de Aon sobre Ciberseguridad y Gestión del Riesgo Ciber en España 2023, entre 2017 y 2020 el número de siniestros de ciberseguros comunicados en España se cuadruplicó.

35 Véase el informe del FSB *Effective Practices for Cyber Incident Response and Recovery*, de octubre de 2020.

36 Véase el informe del FSB *Format for Incident Reporting Exchange (FIRE)*, de abril de 2023.

37 Véase *Principles for Operational Resilience*, de marzo de 2021

regulatorio y su práctica supervisora, y los bancos avanzan en adaptar a los mismos sus políticas, estrategias y marcos de gestión[38].

En el panorama regulatorio internacional se ha iniciado también una discusión sobre si el capital financiero es una medida adecuada para mitigar los ciberriesgos[39]. Por ejemplo, en el escenario de una entidad afectada por un ataque de *ransomware* que cifrara todos sus sistemas críticos, la supervivencia de la entidad dependería de tener o no medidas técnicas que le permitieran recuperarse. El capital financiero no sería el principal elemento de resiliencia en este caso, aunque podría afectar a la capacidad de financiar el despliegue de estas medidas técnicas. En eventos menos extremos, con una pérdida parcial de los sistemas, el beneficio relativo de una mayor solvencia puede ser mayor, al disponer las entidades de más opciones de acción, que requieren de su correspondiente financiación. En cualquier caso, es necesario valorar si la resiliencia adicional frente a ciberriesgos que puede aportar una cierta cantidad de capital financiero puede alcanzarse de forma más eficiente mediante la acumulación de más recursos tecnológicos. Más aún, algunos expertos dudan sobre si los riesgos asociados a la tecnología deberían ser o no una subcategoría del riesgo operacional, dado su carácter transversal a todas las actividades, hecho que se ha exacerbado en paralelo al avance del proceso de transformación digital.

La regulación y la supervisión actúan como catalizadores para que las entidades financieras gestionen adecuadamente el ciberriesgo. Por ello, numerosas jurisdicciones, como la UE, el Reino Unido[40], Estados Unidos[41] o Australia[42] han desarrollado marcos regulatorios y supervisores, así como herramientas en este ámbito.

En la UE, hemos asistido a una intensa actividad regulatoria en materia de ciberriesgos. La publicación en 2016 de la directiva NISD, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información, fue una clara apuesta de la UE para mejorar la ciberseguridad en todos los sectores críticos de un país, incluyendo las entidades de crédito y las infraestructuras de mercado. Esta directiva ha sido revisada y sustituida por la NIS2, que extiende aún más su ámbito de aplicación y que deberá estar transpuesta por los Estados miembros no más tarde de octubre de 2024. Podemos citar otras normas recientes como la Directiva sobre la resiliencia de las entidades críticas[43], el Reglamento de ciberseguridad[44] o el futuro Reglamento de ciberresiliencia[45].

---

38 Véase *BCBS Supervisory newsletter on the adoption of POR and PSMOR*, de noviembre de 2023.

39 L. F. Signorini. (2021). "Implementing Basel III in the EU: remaining challenges and timing". *Eurofi Magazine.*

40 Véase *Operational Resilience of the financial sector* del Banco de Inglaterra.

41 Véase *Cybersecurity and Financial System Resilience Report, CISA Cyber Resilience Review, NIST Cybersecurity Framework.*

42 Véase Council of Financial Regulators. *Cybersecurity.*

43 Directiva UE 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo.

44 Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 («Reglamento sobre la Ciberseguridad»).

45 Propuesta de Reglamento de ciberresiliencia.

Esquema T.1
Principales elementos del Reglamento DORA

FUENTE: Banco de España

El sistema financiero de la UE es el que dispone de mayor cantidad de regulación específica de los ciberriesgos. Entre otras normas sectoriales podemos citar las *Directrices sobre la evaluación del riesgo de TIC* [tecnologías de información y comunicación] *en el marco del PRES* [Proceso de Revisión y Evaluación Supervisora][46], de 2017, y las *Directrices sobre gestión de riesgos de TIC y de seguridad*[47] de la EBA, que se constituyeron en un referente desde su publicación. Las relaciones con terceras partes también han sido foco de atención de la EBA, que publicó en 2019 sus Directrices sobre externalización[48]. En el ámbito de las infraestructuras de mercado, el Banco Central Europeo (BCE) publicó en 2018 sus expectativas de ciberresiliencia[49], sobre la base de las directrices publicadas en 2016 por CPMI-IOSCO.

El Reglamento DORA supondrá un punto de inflexión para la ciberresiliencia del sistema financiero en la UE a partir de su aplicación en enero de 2025. DORA forma parte de la estrategia de finanzas digitales de la Comisión Europea, y su objetivo es mitigar los riesgos asociados a la digitalización y mejorar la resiliencia del sistema financiero europeo. Contiene requerimientos para todas las entidades financieras sobre la gestión de los riesgos asociados

46 Directrices sobre la evaluación del riesgo de TIC en el marco del proceso de revisión y evaluación supervisora (PRES) (EBA/GL/2017/05).
47 Directrices de la EBA sobre gestión de riesgos de TIC y de seguridad (EBA/GL/2019/04).
48 Directrices sobre externalización (EBA/GL/2019/02).
49 Véase el informe del BCE de 2018 Cyber Resilience Oversight Expectations.

a la tecnología, la gestión y la notificación a los supervisores de incidentes tecnológicos, la realización de pruebas sobre la resiliencia de los sistemas, y la gestión de sus relaciones con terceras partes (véase el esquema T.1).

DORA, además de su alcance microprudencial, también trata algunos aspectos de la dimensión sistémica de los ciberriesgos. Así, fomenta el intercambio de información entre instituciones y establece mecanismos de cooperación entre autoridades dentro y fuera del sistema financiero (tanto supervisoras como de otro tipo, tales como agencias de seguridad); ordena un estudio de la viabilidad de un punto único de notificación de incidentes para todas las entidades financieras europeas, y establece un marco de vigilancia sobre aquellos proveedores tecnológicos que sean críticos para el sistema financiero europeo.

En el ámbito de la supervisión microprudencial, las autoridades financieras del sector bancario europeo han incorporado el ciberriesgo tanto al seguimiento continuo y las inspecciones *in situ* de las entidades como a las actividades horizontales. Para ello, se han dotado de recursos especializados y han establecido metodologías y procedimientos de trabajo adaptados a las particularidades de este riesgo. Adicionalmente, la mayor parte de ellas han establecido requerimientos de notificación de ciberincidentes relevantes con el fin de detectar lo antes posible eventos adversos que pudieran requerir algún tipo de intervención por parte de las autoridades.

Además del enfoque estrictamente supervisor, muchas autoridades han establecido marcos de pruebas de ciberresiliencia basadas en inteligencia de amenazas. Estas pruebas tratan de simular un ciberataque sofisticado, y lo más realista posible, sobre los sistemas en producción de una entidad, apoyándose en información de inteligencia sobre los atacantes más probables y sus técnicas y procedimientos. Se trata de valorar las capacidades técnicas, humanas y organizativas de las instituciones para detectar el ataque y reaccionar ante él, sin que los equipos de defensa sean informados previamente de que hay una prueba en curso. La autoridad realiza en todo momento el seguimiento de la prueba para verificar que se cumplen los requisitos del marco. En el caso de la UE, 16 jurisdicciones, entre las que se incluye España, han adoptado ya el marco de pruebas del BCE, TIBER-EU[50].

T.3.2 Gestión del ciberriesgo en las entidades financieras

Como respuesta al incremento del volumen y sofisticación de las ciberamenazas, así como a las exigencias regulatorias y supervisoras, las entidades financieras se esfuerzan en mejorar su gestión del ciberriesgo. Muchas de ellas se apoyan en estándares y buenas prácticas de mercado, así como, en ocasiones, en consultoras especializadas, para evolucionar sus medidas técnicas y mejorar su ciberresiliencia. Esto implica trabajar tanto en los aspectos preventivos y las capacidades de detección como en los procedimientos y soluciones que serán necesarios para responder a un ciberincidente y, si es necesario,

50 Véase la información del BCE sobre el marco TIBER-EU.

recuperarse de su impacto. Dada la complejidad de los sistemas de las entidades y el rápido ritmo de evolución de la tecnología, sostener este esfuerzo en el tiempo supone un reto para muchas, lo que produce niveles de ciberresiliencia heterogéneos.

Las entidades financieras han evolucionado hacia un enfoque más holístico, que pone el foco no solo en la tecnología, sino también en el factor humano y en los aspectos organizativos. Así, a la constante evolución y mejora de las medidas técnicas se ha añadido un significativo esfuerzo de formación y concienciación de sus empleados en materia de ciberseguridad, para tratar de evitar que se conviertan en los vectores de entrada utilizados por los atacantes. Del mismo modo, en los últimos años se observa un mayor conocimiento y comprensión del ciberriesgo entre la alta dirección de las entidades, así como un fortalecimiento de la segunda y la tercera línea de defensa en esta materia, es decir, de las funciones de gestión de riesgos y cumplimiento y la función de auditoría, respectivamente.

En esa misma línea, las entidades financieras han trabajado para concienciar a sus clientes de la importancia de la ciberseguridad. La digitalización de los servicios financieros ha generado un desplazamiento del fraude tradicional hacia los canales digitales, utilizando técnicas de ingeniería social para engañar a los clientes. Las entidades realizan frecuentes campañas de formación y concienciación para ayudar a los clientes a detectar y evitar este tipo de ataques, así como a custodiar y proteger sus credenciales y sus dispositivos, pero esto no es suficiente. Se requiere también la colaboración de otros actores, como los proveedores de telecomunicaciones, por ejemplo, para prevenir ataques basados en la duplicación fraudulenta de tarjetas SIM o campañas de *phishing.*

La ciberresiliencia obliga a establecer como hipótesis de trabajo que los ciberincidentes ocurrirán y que pueden producir interrupciones en los servicios críticos, de las que será necesario recuperarse. Por ello, las entidades establecen y prueban sus planes de continuidad de negocio y contingencia tecnológica, que contemplan diversos escenarios adversos, incluidos los ciberataques. Asimismo, llevan a cabo simulaciones de gestión de crisis para probar si los procedimientos establecidos son adecuados a lo largo de la evolución del incidente que se simula. Algunos de estos ejercicios toman en consideración la concentración en los sectores de proveedores tecnológicos, en particular de servicios en la nube, y la limitación que esto impondría en términos de posibilidad de sustitución ante incidentes.

T.3.3 Evaluación y gestión del riesgo sistémico vinculado a ciberriesgos

De lo individual a lo sistémico

En los últimos años, las autoridades financieras han comenzado a poner también el foco en las implicaciones sistémicas del ciberriesgo. Si bien inicialmente los enfoques regulatorio y supervisor se centraban en la gestión y evaluación del ciberriesgo a nivel individual, el aumento de la dependencia tecnológica del sector, así como del número de

ciberincidentes y su impacto, han hecho necesario abordar el ciberriesgo desde una perspectiva sistémica. Aunque las primeras publicaciones sobre la vertiente sistémica del ciberriesgo son anteriores a 2020[51], a partir de ese año se produce un incremento significativo de los trabajos en la materia.

La JERS creó en 2017 un grupo de trabajo específico para el estudio del potencial impacto del ciberriesgo en la estabilidad financiera, el European Systemic Cyber Group (ESCG). Fruto del trabajo de este grupo, la JERS ha publicado distintos informes que analizan el modelo de propagación del impacto de ciberincidentes que puedan poner en peligro la estabilidad financiera[52] y proponen herramientas para la evaluación y mitigación del ciberriesgo sistémico[53,54].

Los diferentes trabajos y análisis que se han realizado sobre el aspecto sistémico del ciberriesgo comparten una serie de conclusiones relevantes. En primer lugar, la complejidad de evaluar el ciberriesgo y su impacto a nivel sistémico. La cuantificación de impactos es difícil incluso a nivel de una entidad individual, pero la complejidad aumenta en mucha mayor medida al tratar de hacerlo a nivel sistémico. Otro aspecto destacado es la necesidad de que las autoridades dispongan de planes de respuesta ante ciberincidentes sistémicos y someterlos a revisiones y pruebas periódicas. Por último, garantizar una buena coordinación entre autoridades se percibe como un elemento crucial para la gestión de los ciberincidentes sistémicos.

Iniciativas más recientes

En la UE una parte importante de las iniciativas más recientes relacionadas con el componente sistémico del ciberriesgo se centran en la medición de su impacto. Podemos destacar en este ámbito algunos de los trabajos de la JERS, como el desarrollo del concepto de *Systemic Impact Tolerance Objective* (SITO)[55], cuya estimación y análisis para distintas funciones económicas puede ayudar en la compleja tarea de evaluar el ciberriesgo a nivel sistémico. Por ser de aplicación a nivel macroprudencial, los SITO se diferencian de otros conceptos anteriores en el ámbito de la resiliencia y el riesgo tecnológico, como los *Recovery Time Objective* (RTO), medidas estas últimas que representan el tiempo durante el cual una organización individual puede tolerar la falta de funcionamiento de sus sistemas y la caída del nivel de servicio asociada sin que se vea afectada la continuidad del negocio.

Los SITO definen un conjunto de condiciones para las que el sistema financiero en su conjunto no es capaz de absorber el impacto de un ciberincidente sistémico. Establecer

51 Por ejemplo, *Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system* (2017), *Cyber Risk, Market Failures, and Financial Stability (2017), The Future of Financial Stability and Cyber Risk* (2018), *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment* (2019).

52 Véase el informe de la JERS *Systemic cyber risk*, del 19 de febrero de 2020.

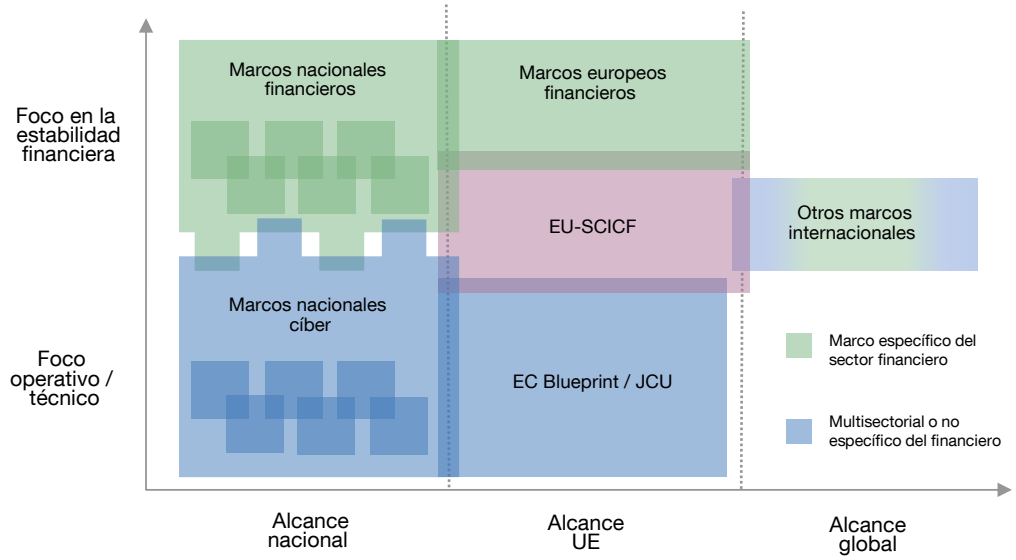
53 Véase el informe de la JERS *Mitigating systemic cyber risk*, del 27 de enero de 2022.

54 Véase el informe de la JERS *Advancing macroprudential tools for cyber resilience*, del 14 de febrero de 2023.

55 Véase el informe de la JERS *Advancing macroprudential tools for cyber resilience*, del 14 de febrero de 2023.

Esquema T.2

Marcos de coordinación de autoridades frente a los ciberriesgos



FUENTE: European Systemic Risk Board. (2022)., Mitigating systemic cyber risk (2022).

estas medidas ayudará a las autoridades a entender las condiciones en las que se puede desencadenar una crisis durante la evolución de un ciberincidente sistémico. Igualmente, contribuirían a establecer umbrales inferiores, de condiciones menos graves, pero asociadas a un cierto nivel de deterioro, para reaccionar y tratar de mitigar los impactos antes de que desemboquen en una crisis de más amplio alcance. Para una función económica determinada, un SITO podría estar definido con base en el número de operaciones afectadas, su valor en euros, la duración del ciberincidente o el número de entidades y jurisdicciones afectadas. De esta forma, en la medida en que un ciberincidente se extendiera a distintas entidades y jurisdicciones (por ejemplo, si todas usaran una misma aplicación que ha sido comprometida por cibercriminales), y su duración fuera potencialmente mayor, se verían afectadas más operaciones y, consecuentemente, el valor en euros. Esto incrementaría el impacto agregado del ciberincidente y se podría llegar a un punto en el que la estabilidad financiera se viera comprometida. La elevada concentración de los proveedores tecnológicos, al limitar las posibilidades de sustitución ante fallos en algunos de ellos, elevaría la probabilidad y velocidad con la que, en determinadas circunstancias, se pueden alcanzar los umbrales SITO, y así la valoración supervisora de estos.

La operacionalización de los SITO plantea algunos retos conceptuales. La JERS ha proporcionado algunos principios para guiar esta tarea. En particular, los SITO deberían reflejar impactos en todas las funciones económicas que pueden verse afectadas por los ciberriesgos y reconocer las interrelaciones entre estas funciones y entre jurisdicciones y sectores de actividad económica. Estas métricas deberían capturar la distinta gravedad y duración de los eventos, y ser también fácilmente comunicables y revisarse periódicamente.

Muy relevante también es la recomendación de la JERS para el establecimiento de un marco pan-europeo de coordinación en caso de ciberincidentes sistémicos (EU-SCICF, por sus siglas en inglés). El objetivo es llenar el vacío detectado entre los marcos de gestión de ciberincidentes a escala europea que ponen el foco en la estabilidad financiera y aquellos específicamente centrados en la respuesta técnica y operativa (véase esquema T.2). El potencial alcance y la velocidad de contagio de los ciberincidentes sistémicos hacían necesario un marco que permitiera una reacción rápida y ágil de las autoridades financieras a escala europea, algo que no parece factible con los existentes actualmente.

La JERS ha elaborado también un trabajo sobre escenarios de pruebas de ciberresiliencia[56] a nivel sistémico. En su informe, la JERS plantea estas pruebas como una nueva herramienta para, entre otras cosas, permitir evaluar la capacidad del sistema financiero para absorber impactos provenientes de ciberincidentes sistémicos con potencial para afectar a la estabilidad financiera. Los escenarios de ciberriesgos para estas pruebas están centrados en cuestiones operativas; difieren así de los escenarios macrofinancieros utilizados en las pruebas de resistencia tradicionales y pueden proporcionar un marco para combinar distintas herramientas y capacidades existentes para gestionar los ciberriesgos.

Por otra parte, el Reglamento DORA anima a las autoridades a organizar ejercicios de gestión de crisis y contingencia que incluyan escenarios de ciberataques. El objetivo es hacer posible gradualmente una respuesta coordinada eficaz a escala de la UE. El BCE está ejecutando en 2024 una prueba de resistencia sobre ciberresiliencia[57] en todas sus entidades supervisadas. También la ejecución de ejercicios sectoriales por parte de autoridades[58] y la industria[59] es ejemplo de la relevancia de estas pruebas.

Herramientas macroprudenciales y otras intervenciones sistémicas de las autoridades financieras frente a ciberriesgos

Las herramientas macroprudenciales contempladas en la normativa vigente del sector bancario no han sido diseñadas específicamente para hacer frente a amenazas externas no financieras, como los ciberriesgos. No obstante, las potenciales consecuencias disruptivas[60] de un ciberincidente para el conjunto del sistema financiero podrían llegar a justificar la liberación de colchones de capital macroprudenciales previamente acumulados, a fin de facilitar que las entidades puedan continuar con la provisión de crédito a la economía. Así, el instrumental macroprudencial podría ser susceptible de adaptación para hacer frente

56 *Cyber Resilience Scenario Testing* (CyRST).

57 Véase la nota de prensa del BCE *ECB to stress test banks' ability to recover from cyberattack.*

58 Por ejemplo los ejercicio llevados a cabo por el Banco de Inglaterra junto con la industria (SIMEX), *SIMEX 22 – A two-day market wide simulation exercise to test the UK financial sector's resilience to a major operational disruption*.

59 Por ejemplo los ejercicios organizados en España por el Centro de Cooperación Interbancaria o el ISMS Forum ISMS Forum pone a prueba las capacidades de ciberresistencia de 35 compañías españolas a través de los Ciberejercicios Multisectoriales.

60 Más allá de las dificultades operativas iniciales que pueden causar, los ciberincidentes también merman como consecuencia de estas la rentabilidad de las entidades financieras y, potencialmente, su liquidez y solvencia. Así, en el periodo posterior a un ciberincidente, la oferta de crédito podría verse perjudicada.

a ciberriesgos. Por ejemplo, el uso del colchón contra riesgos sistémicos podría permitir discriminar entre entidades bancarias en función de su grado de sistemicidad tecnológica. Todo ello podría contribuir a limitar la ocurrencia de eventos sistémicos y consiguientes fenómenos de contagio. Esta es, no obstante, una cuestión cuyo análisis se encuentra en una fase muy preliminar y requiere todavía de un esfuerzo de investigación notable para poder adoptar recomendaciones de política más definidas.

La materialización de ciberincidentes con un impacto financiero notable puede exigir el despliegue de instrumentos financieros para la gestión de crisis. La gestión de una crisis financiera, con independencia de su origen, puede abordarse con instrumentos ya existentes, como la garantía de depósitos, moratorias o inyecciones especiales de liquidez, adaptando, eso sí, las condiciones de su utilización al contexto tecnológico y de riesgo. Así, un ciberincidente podría provocar que una entidad viese limitada su operativa y causarle problemas de liquidez. La provisión de liquidez por parte de los bancos centrales a las entidades solventes pero que, a causa del ciberincidente, han dejado de tener liquidez podría permitir a las entidades continuar con su actividad, ayudando a mitigar el riesgo que el incidente pudiera implicar sobre la estabilidad financiera y permitiendo continuar con la prestación del servicio a la economía.

En el mismo sentido, los marcos de resolución de las entidades bancarias también pueden ser efectivos en estos escenarios. Los planes de resolución y recuperación, aunque no están diseñados específicamente para estas situaciones, pueden ser adaptados para asegurar la continuidad de las funciones críticas de las entidades que pudieran estar afectadas por el incidente.

Conviene destacar la necesidad de adaptar las condiciones de aplicación de los instrumentos financieros al contexto tecnológico de los riesgos[61]. Las disrupciones simultáneas en los ámbitos operativo y financiero justifican enfoques combinados de actuación. La disponibilidad del capital tecnológico adecuado puede ser condición necesaria para poder aplicar recursos financieros tradicionales (por ejemplo, la liquidez de emergencia y el marco de resolución antes comentados) ante estos ciberincidentes. Este capital tecnológico se refiere al conjunto de *software, hardware,* conocimientos y personal especializado que permite gestionar de forma eficaz y eficiente los sistemas de información de las entidades y, en particular, garantizar su seguridad y ciberresiliencia. El incremento del capital tecnológico puede ser la opción más eficiente para limitar los ciberriesgos sistémicos, al reducir marcadamente su impacto financiero[62]. La inversión en la modernización y sustitución de sistemas de información *legacy,* provenientes de periodos pasados, es particularmente prioritaria en este sentido.

---

61 Véase José Ramón Martínez Resano. (2022). *Digital Resilience And Financial Stability. The Quest For Policy Tools In The Financial Sector*.

62 Por ejemplo, un ciberincidente que cause una parálisis completa del sistema financiero tiene un elevado coste económico por unidad de tiempo. La inversión en el capital tecnológico que reduzca su probabilidad de ocurrencia puede ser más eficiente, y factible, que la acumulación de capital equivalente a las pérdidas en estos tipos de incidentes.

Dos posibles ejemplos que se han de explorar son la introducción de circuit-breakers y el recurso a mecanismos colectivos de apoyo entre las entidades que permitan al sistema en su conjunto compartir capital tecnológico. La primera medida supone la interrupción de procesos en crisis tecnológicas y financieras simultáneas. Esta pausa permite recabar mayor información sobre el episodio de crisis y adaptar mejor a ella la respuesta operativa y financiera. La segunda permitiría implementar redundancia y seguridad en el sistema, haciendo así posible la reconducción colaborativa de procesos entre entidades en caso de fallo de una o, similarmente, el acceso a datos *(data vault)* comprometidos en un ciberataque individual.

T.4 Conclusiones y perspectivas futuras

La digitalización de la sociedad, la economía y el sistema financiero continuarán a un ritmo acelerado, lo que obligará a todos los actores en el sistema financiero, incluidas las autoridades supervisoras y regulatorias, a intensificar sus esfuerzos en materia de ciberriesgo. Esta adaptación requerirá incorporar a las organizaciones los perfiles técnicos necesarios en un número suficiente, por lo que la captación y la retención del talento seguirán siendo un reto para el sector, especialmente para las entidades más pequeñas.

El potencial de la inteligencia artificial brindará nuevas herramientas tanto a los ciberatacantes como a los equipos de defensa. Las capacidades de generación de contenidos, tanto texto como voz o imágenes, facilitarán la suplantación de identidades y harán mucho más creíbles los ataques de ingeniería social. Asimismo, la inteligencia artificial puede ayudar a la creación de *malware* o a la optimización de los ataques. Por otro lado, permite a los equipos defensivos identificar de manera temprana las ciberamenazas, mediante el reconocimiento de patrones a partir del análisis de grandes volúmenes de información en tiempo casi real. También es posible automatizar parcialmente la respuesta, complementando así la labor de los analistas y acortando sustancialmente los tiempos de reacción.

Las posibilidades que brinda la computación cuántica[63] hacen que a medio plazo una gran parte de los sistemas de cifrado actuales puedan ser vulnerados. Esto afectaría a la confidencialidad de la información cifrada, incluyendo las copias de seguridad, por lo que los robos actuales de datos cifrados podrían proporcionar al atacante información descifrada en el futuro. Pero también afectaría a la mayor parte de los mecanismos de autenticación y, por tanto, a la integridad de la información, ya que se podrían crear credenciales falsas y obtener ilegítimamente claves privadas auténticas. De este modo, se podría llegar a la alteración de la historia legal mediante la manipulación de documentos firmados o la creación de documentos falsos con firmas válidas. Se está trabajando[64] ya en la creación de algoritmos criptográficos

63 *Quantum computing,* por su término en inglés. Este paradigma de computación utiliza las leyes de la mecánica cuántica para resolver problemas complejos que no pueden ser resueltos con sistemas clásicos.

64 Véase el concurso organizado por el *National Institute of Standards and Technology* estadounidense para establecer estándares de criptografía post-cuántica.

resistentes a la computación cuántica y en planificar la migración a dichos algoritmos de los elementos de *hardware, software* y servicios que usan criptografía potencialmente vulnerable.

Desde la perspectiva de la ciberresiliencia del sistema financiero, hay iniciativas encaminadas a garantizar la recuperación de los datos críticos en caso de un incidente grave. Las denominadas «estrategias de *data vaulting*» plantean el almacenamiento fuera de línea y fuera de las instalaciones de los datos que una entidad necesita para operar sus servicios críticos. El ejemplo más avanzado es *Sheltered Harbor*[65], participado y apoyado por las principales asociaciones bancarias estadounidenses. Las entidades participantes envían su información encriptada y en un formato acordado a instalaciones de *data vaulting* comunes, de modo que, en caso de contingencia mayor sus datos puedan ser recuperados y procesados en una plataforma de recuperación. Los potenciales requisitos micro- y macroprudenciales sobre *data vaulting* podrían constituir un elemento útil para la regulación y supervisión de los ciberriesgos, pero esta es una cuestión todavía incipiente.

La compartición de información de ciberamenazas y ciberincidentes es clave para mejorar las capacidades colectivas de defensa. La información técnica sobre los datos de un ciberataque que ha tenido impacto en una entidad puede ayudar a otras a protegerse frente a un ataque similar. En el sistema financiero existen ya numerosos foros de intercambio de información, tanto específicos de la industria[66] como con participación de autoridades[67]. La posición central de estas últimas, que bajo DORA recibirán notificaciones de ciberincidentes de las entidades sobre las que tienen competencia, les permitirá devolver al sector información de utilidad.

Del mismo modo, la realización de pruebas de ciberresiliencia y ejercicios de gestión de crisis sectoriales e incluso con participación de diversos sectores será también crítica en los próximos años. Será necesario garantizar no solo la capacidad de respuesta y recuperación de cada entidad financiera, sino la del sistema en su conjunto, para lo que será imprescindible la realización de pruebas sectoriales que incluyan la participación de los proveedores relevantes. Idealmente, a futuro se deberían incorporar a estas pruebas otros sectores respecto a los que existen interdependencias operativas. La incorporación se realizaría de manera progresiva a medida que dichos sectores alcancen un nivel de madurez adecuado. Las autoridades tendrán que desempeñar un papel de coordinación fundamental en caso de una crisis, por lo que su impulso e implicación en la realización de estos ejercicios son claves.

Es necesario seguir avanzando en la cuantificación y comprensión de los ciberriesgos para la estabilidad financiera y el potencial papel de las políticas macroprudenciales en su mitigación. Las interconexiones financieras son un objeto complejo de análisis, y el proceso de digitalización ha extendido estas redes con nuevos actores, como son los

65 Véase el sitio web Sheltered Harbor.

66 Por ejemplo, FS-ISAC.

67 Por ejemplo, la plataforma CIISI-EU *(Cyber Information and Intelligence Sharing Initiative).*

proveedores tecnológicos. Esta transformación exige evaluar el potencial papel en la mitigación de ciberriesgos de las medidas macroprudenciales tradicionales (por ejemplo, cochones de capital) y también en qué medida los requisitos sobre los recursos tecnológicos (por ejemplo, *data vaulting,* pruebas de resiliencia operacionales) pueden representar un sustituto más eficaz y eficiente de estas.