Fortaleciendo la ciberresiliencia del sector financiero. Evolución y tendencias

Silvia Senabre, Iván Soto y José Munera

BANCO DE ESPAÑA

Los autores pertenecen a la Dirección General de Supervisión del Banco de España, y agradecen los comentarios recibidos de un evaluador anónimo. Dirección de correo electrónico para comentarios: silvia(dot)senabre(at)bde(dot)es.

FORTALECIENDO LA CIBERRESILIENCIA DEL SECTOR FINANCIERO. EVOLUCIÓN Y TENDENCIAS

Resumen

El debate alrededor de la ciberresiliencia del sector financiero ha cobrado especial relevancia en los últimos años. En este artículo los autores tratan de aclarar qué se entiende por este concepto y por qué constituye una preocupación creciente para las entidades financieras y para las autoridades. Analizan cómo ha evolucionado la ciberresiliencia del sector financiero en los últimos años, cuál es la situación actual y qué tendencias se observan. Por último, definen la manera en que los distintos actores involucrados trabajan para contribuir a fortalecerla. En particular, detallan las distintas actuaciones regulatorias y supervisoras que en este ámbito desarrollan las autoridades sectoriales.

Palabras clave: resiliencia, resiliencia operacional, ciberresiliencia, ciberseguridad, ciberincidente.

1 Introducción

En los últimos años las referencias a la resiliencia se han convertido en elemento habitual de todo tipo de publicaciones, discursos[1] y debates, por parte tanto de las autoridades como del sector privado, tendencia que se ha exacerbado aún más en el contexto de la pandemia de COVID-19. Pero ¿a qué se refieren con este concepto?

Conviene comenzar aclarando que el término *resiliencia* es originario del ámbito de la psicología y que, aunque no existe una única definición para él, suele entenderse como la capacidad de adaptación ante una situación adversa. Partiendo de este concepto general, se han ido derivando distintos términos para su uso en otros ámbitos. Uno de los más utilizados, especialmente relevante desde la perspectiva adoptada en este artículo, es el de *resiliencia operacional,* que el Comité de Supervisión Bancaria de Basilea (BCBS, por sus siglas en inglés) definió en sus *Principles for Operational Resilience*[2] como la capacidad de un banco para mantener sus operaciones críticas en situaciones adversas[3], definición que podría aplicarse no solo a bancos, sino también a todo tipo de compañías privadas e instituciones públicas dentro y fuera del sector financiero.

1 Véase Hernández de Cos (2019).

2 Véase Comité de Supervisión Bancaria de Basilea (2021a).

3 Del original en inglés: *The Committee defines operational resilience as the ability of a bank to deliver critical operations through disruption.*

No resulta extraño que, en un mundo cada vez más digitalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un rol esencial en la operativa financiera, haya surgido el concepto de *ciberresiliencia,* como caso particular de resiliencia operacional. En este artículo se tomará como referencia el *Cyberlexicon*[4] del Consejo de Estabilidad Financiera (FSB, por sus siglas en inglés), que 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*[5]. Esta definición aúna tanto el componente de *ciberseguridad,* más preventivo, como el de continuidad de negocio, enfocado a la respuesta y recuperación cuando los incidentes ocurren.

Conviene destacar que la propia definición de *ciberincidente* en el *Cyberlexicon* del FSB remite tanto a los de naturaleza maliciosa, causados por ciberataques, como a los no maliciosos. Estos últimos, que incluyen eventos como desastres naturales, errores humanos o fallos accidentales en los sistemas, también pueden afectar a la capacidad de las entidades y del sector para seguir operando con normalidad, por lo que la resiliencia frente a estos ciberincidentes es igualmente relevante. Sin embargo, el artículo profundizará más en los intencionados, dado su mayor impacto potencial.

El sector financiero constituye un ecosistema muy complejo, formado por numerosos participantes —entre los que podemos nombrar infraestructuras de mercado, entidades financieras y proveedores—, fuertemente interconectados y dependientes entre sí, y en los que se pueden observar distintos niveles de madurez en materia de ciberresiliencia.

Algunas de las características intrínsecas del sector financiero no solo generan un elevado nivel de exposición de las entidades individuales a los ciberincidentes, sino que además facilitan que su impacto se pueda extender y amplificar hasta poner en peligro la estabilidad financiera[6]. Entre estas características podemos citar su fuerte dependencia de la tecnología, su atractivo para atacantes con distintas motivaciones, el alto grado de interconexiones entre sus integrantes, y una gran sensibilidad a la pérdida de la confianza de sus participantes[7].

Por este motivo, mejorar la ciberresiliencia del sector financiero es un elemento imprescindible para el mantenimiento de la estabilidad financiera. A lo largo del artículo se expondrán algunas de las principales iniciativas que tanto el sector

4 Véase Consejo de Estabilidad Financiera (2018).

5 Del original en inglés: *The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.*

6 Véase Herrera, Munera y Williams (2021).

7 Véase Junta Europea de Riesgo Sistémico (2020).

privado como las autoridades han llevado a cabo o tienen en curso para contribuir a este objetivo, haciendo especial hincapié en aquellas que afectan directamente al sector financiero español.

2 Contexto

2.1 Digitalización y superficie de exposición

Históricamente, el sector financiero ha sido muy proactivo en la utilización de las tecnologías de la información para habilitar nuevos modelos de negocio y optimizar procesos internos. En los últimos años este proceso de transformación digital se ha acelerado extraordinariamente, y se ha convertido en imprescindible para la supervivencia de las entidades, por distintos motivos.

En primer lugar, cabe mencionar los cambios en las expectativas de los clientes, que valoran disponer de servicios flexibles que configuren una oferta personalizada y acceder a estos de forma inmediata, desde cualquier lugar y con cualquier dispositivo. Este fenómeno se ha visto reforzado por la aparición de nuevos competidores para las entidades tradicionales, como son las *bigtech*[8] o las *fintech*[9], que ofrecen a los clientes soluciones muy atractivas y son muy ágiles haciendo evolucionar su oferta.

Además, el entorno económico de bajos tipos de interés ha impulsado a las entidades a adaptar su modelo de negocio, buscando fuentes de ingreso alternativas mediante el lanzamiento de nuevos productos y servicios, y reduciendo costes a través de la mejora de la eficiencia de sus procesos internos. Todo ello aprovechando la rápida evolución de la tecnología, que ha permitido multiplicar las capacidades de los sistemas a la vez que se reducía su precio.

Como consecuencia, el sector financiero está fuertemente digitalizado, hasta el punto de que las entidades son completamente dependientes de su tecnología, que no solo es un instrumento facilitador para el negocio, sino que se ha convertido en un factor diferencial y competitivo. Evidentemente, el elevado nivel de digitalización aumenta el riesgo de que ocurran ciberincidentes, tanto causados por fallos en los sistemas como de origen malicioso o ciberataques. A este incremento del riesgo contribuyen, entre otros factores, la complejidad del entorno tecnológico de la mayor parte de las entidades financieras, donde conviven aplicaciones antiguas con otras que se apoyan en tecnologías más innovadoras, fruto no solo de los procesos

8 Según el FSB, «*BigTech* firms are large technology companies with extensive established customer networks».

9 El FSB define *fintech* como «technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services».

de transformación, sino también de las distintas fusiones y adquisiciones que conforman la historia reciente del sector financiero español. 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.

Es importante señalar que, para llevar a cabo estos procesos de transformación digital y tener acceso a las innovaciones tecnológicas que más pueden contribuir a su negocio, las entidades financieras complementan sus capacidades mediante la contratación de servicios de proveedores, inversiones en *start-ups* o adquisiciones de productos de terceros. También participan en incubadoras[10] y aceleradoras[11] o colaboran en consorcios.

Por esta razón, la resiliencia y la ciberseguridad de estas terceras partes, y en especial de los proveedores, se han convertido en una preocupación creciente para autoridades y entidades. De hecho, algunos de estos proveedores han pasado a ser elementos vertebradores para el sector financiero, a un nivel comparable al de las infraestructuras de mercado y las entidades sistémicas. 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.

Conviene destacar que, a la lista de los grandes proveedores comúnmente considerados como sistémicos, hay que añadir proveedores de nicho menos conocidos y otras dependencias de terceros no debidamente identificadas, producidas por las subcontrataciones sucesivas a lo largo de la cadena de externalización.

En este contexto, la pandemia de COVID-19 ha actuado como un catalizador, acelerando los procesos de digitalización que ya estaban en marcha en las entidades financieras, e incrementando aún más su dependencia de proveedores de servicios tecnológicos.

Por un lado, las entidades se han visto obligadas a ampliar su oferta de servicios financieros a distancia, lo que ha aumentado la exposición de sus clientes a ataques, y se han observado crecimientos muy significativos en los casos de *phishing*[12],

10 Las incubadoras ofrecen a los emprendedores y *start-ups* en sus primeras fases de vida un espacio físico con servicios básicos como las telecomunicaciones, en el que poner en marcha una idea de negocio innovadora. Generalmente dan acceso a una red de contactos y a equipos de expertos, que les asesoran para materializar su proyecto.

11 Las aceleradoras se encargan de acompañar a *start-ups* ya en funcionamiento (a diferencia de las incubadoras, que ayudan a *start-ups* en sus primeras fases de vida y les facilitan servicios básicos). Las aceleradoras ayudan a impulsar el crecimiento de las *start-ups* actuando como mentores en la definición de su modelo de negocio, su estrategia comercial e incluso la captación de financiación.

12 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.

vishing[13] y suplantación de sitios web y aplicaciones móviles, entre otros. Aunque las entidades han realizado y realizan esfuerzos importantes 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.

Por otro lado, los elevados niveles de teletrabajo han traído consigo riesgos adicionales para las entidades y sus empleados, entre los que podemos citar los originados por el despliegue de nueva infraestructura tecnológica y la rápida implantación de soluciones de trabajo colaborativo, los accesos insuficientemente securizados a sistemas corporativos desde dispositivos personales y redes de conexión domésticas, así como el manejo de datos confidenciales en los domicilios de los empleados. Todo ello ha generado un aumento de la exposición de las entidades a ciberamenazas, situación que se ha visto agravada como consecuencia de la premura impuesta por las circunstancias, que en ocasiones ha llevado a la relajación de ciertos controles o análisis de seguridad adecuados para poder seguir operando.

Además, la necesidad repentina de aumentar la capacidad de sus sistemas forzó a muchas entidades a adquirir servicios externos adicionales, lo que ha incrementado su dependencia de terceros, y en particular de proveedores de servicios en la nube. Este es un mercado fuertemente concentrado en un número relativamente pequeño de proveedores, de modo que cualquier incidente en uno de ellos puede tener impacto inmediato en múltiples entidades cliente.

La conjunción de estos factores ha creado un entorno muy atractivo para los ciberatacantes, que no han perdido la oportunidad de explotarlo. Así, se ha podido observar que durante la pandemia el sector financiero ha sido la principal víctima de ciberataques en todo el mundo, solo superada por el sector sanitario[14].

Es preciso señalar que, aunque algunos estudios sugieren que el financiero es uno de los sectores críticos mejor preparados frente a los ciberriesgos, en parte debido a su elevado grado de regulación y supervisión, el nivel de ciberresiliencia de sus integrantes no es homogéneo. En algunos casos, las medidas de seguridad y los controles implementados por las entidades, especialmente en el caso de las más pequeñas, no resultan suficientes para gestionar los ciberriesgos que la pandemia ha exacerbado. No es de extrañar, por tanto, que, entre las entidades que han sufrido un mayor incremento en el número de ciberataques recibidos, destaquen las cooperativas de crédito, las entidades de pago y las aseguradoras, pertenecientes a sectores que concentran muchas entidades de pequeño tamaño[15].

---

13 El *vishing* es un tipo de estafa de ingeniería social por teléfono en el que, 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.

14 Véase Banco de Pagos Internacionales (2021).

15 *Ibidem.*

Además de los ciberataques atribuidos al crimen organizado, que persiguen un beneficio económico, se ha observado también un incremento de los ciberataques con motivaciones geopolíticas, algunos de los cuales han sido sumamente sofisticados y se han dirigido contra distintos proveedores de la cadena de suministro.

2.2 El sistema financiero ante las tensiones geopolíticas

Desde que disponemos de registros históricos, el escenario económico y financiero ha sido tanto causa de conflictos como objetivo en confrontaciones. La seguridad de los Estados siempre ha tenido un carácter multidimensional, donde, además de los conceptos militares, los aspectos sociales, políticos o —los que aquí nos ocupan— económicos y financieros han sido y siguen siendo de vital importancia. El sistema financiero, en su rol de canalizar los recursos económicos y actuar como motor para el tejido empresarial productivo, constituye un elemento fundamental para el desarrollo de las economías. Por este motivo, en el campo de la geopolítica, el sector financiero de los adversarios ha pasado a ser un objetivo prioritario para los enemigos de cualquier Estado.

Durante las últimas décadas el *ciberespacio*[16] se ha convertido en un dominio más que sumar a los tradicionales de tierra, mar, aire y espacio, como medio para el ataque y la defensa de objetivos. Los Estados invierten cada vez más recursos en desarrollar sus capacidades en este ámbito, tanto en la vertiente defensiva como en la ofensiva.

Desde la perspectiva de la defensa, la ciberresiliencia y la protección de las infraestructuras críticas del sector financiero son aspectos reflejados en las estrategias de seguridad nacional de un número cada vez mayor de países, entre ellos España[17]. Como referencia de la madurez en materia de ciberseguridad y ciberresiliencia, la Unión Internacional de Telecomunicaciones, agencia especializada de las Naciones Unidas para las TIC, publica anualmente un índice global de ciberseguridad, que en su edición de 2020[18] sitúa España como uno de los países con una mayor capacidad en dicho sentido, ya que ocupa el cuarto lugar de la lista.

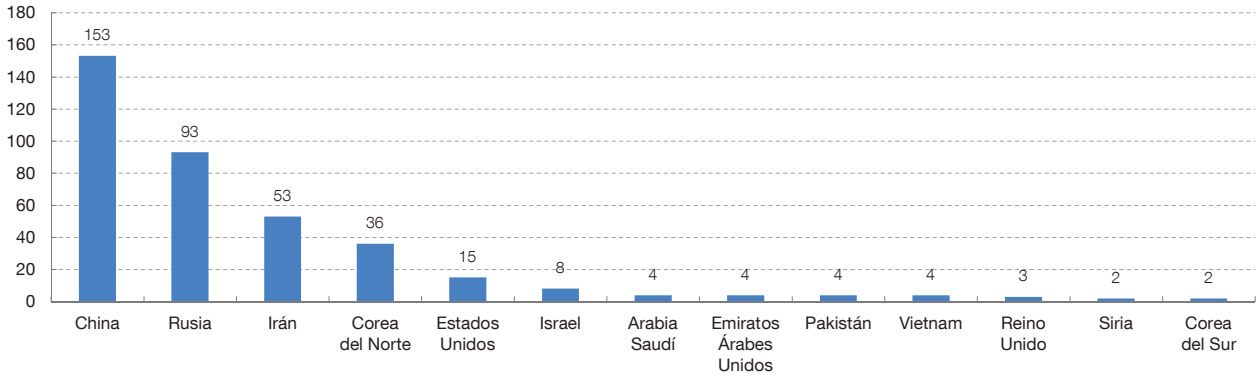
En cuanto al componente ofensivo, es habitual la organización de grupos especializados y operativos, tanto integrados en las estructuras militares como financiados y organizados al margen de estas, encargados de lanzar ataques contra

16 NIST define *ciberespacio* como "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".

17 Véase Departamento de Seguridad Nacional (2017 y 2019).

18 Véase Unión Internacional de Telecomunicaciones (2021).

Gráfico 1
ESTIMACIÓN DEL NÚMERO DE CIBERATAQUES PATROCINADOS POR ESTADOS (2005-2020)



FUENTE: Council on Foreign Relations (2021).

otras potencias en el ciberespacio. Desde 2005, se sospecha que al menos treinta y cuatro países han patrocinado ciberataques. Entre ellos, tal y como se muestra en el gráfico 1, se estima que China, Rusia, Irán y Corea del Norte patrocinaron el 77 % de todas las operaciones sospechosas[19], y, por sus medios e inversión, se espera que sigan siendo los actores más activos en el futuro, si bien también algunas potencias occidentales, como Estados Unidos, el Reino Unido o Israel, desempeñan un papel muy relevante en este ámbito.

Generalmente se utiliza el término *state sponsored actors* para referirse a este tipo de grupos estatales, que tienen como prioridades, junto al ciberespionaje y las operaciones de influencia, el ciberataque a las infraestructuras críticas de otros Estados, entre las que el sector financiero se ha convertido en un objetivo preferente. Así, en el *Informe Anual de Seguridad Nacional 2019,* emitido por el Departamento de Seguridad Nacional[20], se indica que en España el 54 % de los ciberataques contra infraestructuras críticas se dieron en el sector financiero y tributario.

Los grupos estatales tienen un alto nivel de respaldo económico, que les permite contar con personal altamente cualificado y con capacidades ofensivas avanzadas. Si bien, comparativamente, sus ciberataques son menos frecuentes, su impacto es potencialmente superior al de las campañas realizadas por actores no estatales, como pueden ser *hacktivistas*[21] o cibercriminales.

No en vano, uno de los principales objetivos perseguidos por estos grupos es desestabilizar los Estados que atacan, y quebrar la confianza en el sistema financiero

19 Véase Council on Foreign Relations (2021).

20 Véase Departamento de Seguridad Nacional (2021).

21 *Hacktivismo* (término compuesto de *hacker* y activismo), también conocido como *ciberactivismo,* hace referencia a la utilización de herramientas y ataques digitales con fines políticos.

es un medio muy eficaz de conseguirlo. Aprovechando el alto grado de interconexión entre los distintos integrantes del sector financiero, los atacantes buscan generar ciberincidentes que puedan propagarse, escalar en magnitud y generar consecuencias sistémicas a gran velocidad. En este sentido, tanto el Banco Central Europeo (BCE) como la Junta Europea de Riesgo Sistémico (ESRB, por sus siglas en inglés) han advertido de la existencia de canales plausibles a través de los cuales un ciberincidente podría transformarse en una grave crisis financiera[22].

Por su naturaleza, los activos manejados por las entidades financieras son fácilmente monetizables (si no lo son directamente), por lo que constituyen un objetivo especialmente atractivo para los ciberatacantes. Algunos de los grupos estatales más dañinos, como es el caso de los respaldados por Corea del Norte, son especialmente activos lanzando ciberataques que buscan la realización de transferencias fraudulentas[23], el robo de criptodivisas o la obtención de un rescate a cambio de devolver a sus víctimas la información cifrada por los atacantes y no divulgarla *(ransomware*[24]). Tal y como reconoce el Consejo de Seguridad de las Naciones Unidas[25], estos grupos se han convertido en una fuente más de financiación para los Estados que los promocionan, y en un modo práctico de esquivar, o al menos mitigar, el efecto de las sanciones económicas internacionales. 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.

Por último, y como se ha mencionado antes, ha crecido el número y la sofisticación de los ciberataques a terceras partes. Como ejemplo paradigmático en cuanto a las consecuencias de estos, podemos citar el caso de SolarWinds. En diciembre de 2020 se descubrió que un *software*[26] distribuido por la compañía SolarWinds había sido alterado por un grupo de ciberatacantes para que instalara un troyano[27] en todos los clientes que usaban este producto. Entre los afectados podemos citar numerosas agencias federales estadounidenses, así como la OTAN, el Parlamento Europeo o compañías como Microsoft, además de otras empresas de distintos sectores, incluido el financiero, en todo el mundo. Este ciberataque, atribuido a los servicios de inteligencia rusos, extremadamente sofisticado y que consiguió pasar inadvertido durante meses, es un ejemplo perfecto de la amplificación que pueden tener los ciberataques a la cadena de suministro. A pesar del tiempo y de los

22 Véase Junta Europea de Riesgo Sistémico (2020).

23 Ataque al Bangladesh Bank (banco central de Bangladés), en el que se realizaron transferencias fraudulentas a través de SWIFT por valor de más de 80 millones de dólares.

24 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.

25 Véase Naciones Unidas (2019).

26 En concreto, el *software* denominado ORION, utilizado por los clientes para monitorizar su infraestructura tecnológica.

27 En informática, se denomina *caballo de Troya,* o *troyano,* un programa aparentemente legítimo e inofensivo, que, al ejecutar, brinda al atacante el acceso remoto al equipo infectado.

recursos necesarios para preparar y ejecutar una operación de esta envergadura, los atacantes han conseguido infiltrarse en miles de organizaciones y empresas de relevancia a través de un único punto de entrada, multiplicando extraordinariamente la eficacia y eficiencia de su ataque.

3 Ciberresiliencia y sector financiero

3.1 Evolución de la ciberresiliencia en el sector financiero

Aunque el uso de los términos *resiliencia* y *ciberresiliencia* no se extiende en el sector financiero hasta 2016, esto no quiere decir que hasta esa fecha no existiera la preocupación, tanto entre las autoridades como entre las propias entidades, por gestionar los riesgos que pudieran tener un impacto en la resiliencia de las entidades y, más concretamente, en su vertiente tecnológica.

Si nos remontamos a 2005, vemos que en el sector financiero empezaba a generalizarse la preocupación por el riesgo tecnológico y la continuidad de negocio, ambos dentro del ámbito más general de la gestión del riesgo operacional. El foco estaba fundamentalmente en la tecnología, y por parte de las autoridades la perspectiva era microprudencial. En esta línea, en 2007 el Banco de España comenzó a realizar las primeras inspecciones *in situ* para analizar la situación de la tecnología y la gestión de sus riesgos asociados en las entidades supervisadas; para ello desarrolló una primera metodología al efecto, que posteriormente ha ido mejorando.

Desde entonces se ha producido una evolución significativa de los conceptos, paralela a la creciente digitalización del sector y al incremento en la conciencia de la relevancia de estos riesgos no financieros. A modo de ejemplo, la primera versión de los *Principles for the Sound Management of Operational Risk* publicada en 2011[28] por el BCBS contenía una sola vez la palabra *resiliencia* y ninguna el prefijo *ciber,* mientras que la revisión de estos principios publicada en 2021[29] menciona hasta 22 veces *resiliencia,* usa el prefijo *ciber* en 8 ocasiones y contiene un nuevo principio sobre la gestión de los riesgos asociados a la tecnología.

En los últimos años se ha hecho patente que la ciberresiliencia es una preocupación global que precisa de la cooperación de todos los actores implicados, lo que ha llevado a la aparición de numerosos foros de debate y colaboración tanto en el ámbito de la industria como entre autoridades, y a un esfuerzo regulador y normativo muy relevante. Además, se ha producido un desplazamiento hacia un

28 Véase Comité de Supervisión Bancaria de Basilea (2011).

29 Véase Comité de Supervisión Bancaria de Basilea (2021b).

enfoque más holístico, que no se centra exclusivamente en gestionar la tecnología, sino que concede la misma importancia a las personas y los procesos de las organizaciones, y enlaza con disciplinas ya existentes, como la continuidad de negocio.

En el año 2014 la Autoridad Bancaria Europea empezó a analizar la situación regulatoria y supervisora de los riesgos tecnológicos en las diferentes jurisdicciones europeas. Desde entonces, esta misma autoridad ha creado grupos de trabajo especializados y ha publicado abundante normativa que ha tenido un gran impacto en el sector, entre la que podemos destacar las *Directrices sobre la evaluación del riesgo de TIC en el marco del proceso de revisión y evaluación supervisora,* de 2017[30], las *Recomendaciones sobre la externalización de servicios a proveedores de servicios en la nube,* también de 2017[31] (posteriormente embebidas en las *Directrices sobre externalización,* de 2019[32], y derogadas en su forma original), y las *Directrices de la ABE sobre gestión de riesgos de TIC y de seguridad,* de 2019[33].

También en el año 2014 comienza su actividad el Mecanismo Único de Supervisión, centrado en el BCE como supervisor bancario del área del euro, que desde el principio prestó especial atención al riesgo tecnológico. No solo desarrolló capítulos *ad hoc* en el manual de la supervisión para su uso durante las inspecciones *in situ* específicas para este riesgo, sino que también elaboró una metodología para la valoración continuada de dicho riesgo en el proceso de revisión y evaluación supervisora. Además estableció un procedimiento para la notificación de ciberincidentes relevantes por parte de las entidades y realiza diversos análisis horizontales sobre aspectos relacionados con el riesgo tecnológico y su gestión, parte de cuyos resultados comparte con la industria[34].

La publicación en 2016 por parte de CPMI-IOSCO[35] de la *Guidance on cyber resilience for financial market infrastructures*[36] y en 2018 del *discussion paper Building the UK Financial Sector's Operational Resilience*[37] por parte del Banco de Inglaterra constituyó un punto de inflexión, a partir del que se empezó a generalizar en el sector la discusión sobre los conceptos de *resiliencia operacional* y *ciberresiliencia.* La idea subyacente es que no es suficiente con poner medidas

30 *Directrices sobre la evaluación del riesgo de TIC en el marco del proceso de revisión y evaluación supervisora (PRES) (EBA/GL/2017/05)*.

31 *Recomendaciones sobre la externalización de servicios a proveedores de servicios en la nube (EBA/REC/2017/03)*.

32 *Directrices sobre externalización (EBA/GL/2019/02)*.

33 *Directrices de la ABE sobre gestión de riesgos de TIC y de seguridad (EBA/GL/2019/04)*.

34 Véase Banco Central Europeo (2021).

35 Siglas en inglés del Comité de Pagos e Infraestructuras del Mercado y la Organización Internacional de Comisiones de Valores.

36 Véase CPMI-IOSCO (2016).

37 Véase Banco de Inglaterra (2018).

preventivas para tratar de impedir la ocurrencia de ciberincidentes, sino que hay que asumir que ocurrirán y estar preparados para gestionarlos de modo que su impacto se minimice y se puedan seguir prestando las funciones y servicios considerados críticos.

Desde 2018 se ha intensificado la publicación de todo tipo de trabajos y normativa sobre ciberresiliencia. Algunos ejemplos destacados son la publicación en 2018 del *Cyberlexicon,* del FSB, de las *Cyber Resilience Oversight Expectations*[38], del BCE, y del informe *Cyber-resilience: range of practices*[39], del BCBS. Este último también ha publicado en 2021 los *Principles for Operational Resilience,* que han despertado mucho interés en el sector.

Más allá del ámbito regulador, también las iniciativas para la supervisión de estos riesgos han crecido significativamente en los últimos años. La mayor parte de las autoridades se han dotado de recursos especializados, incorporándolos tanto al seguimiento continuo y las inspecciones *in situ* de las entidades como a las actividades horizontales sobre el conjunto del sector.

El Banco de España es uno de los supervisores europeos con más capacidad y más experiencia en este ámbito. Por esta razón ha contribuido y contribuye de manera muy relevante al desarrollo de las principales iniciativas reguladoras y normativas europeas y mundiales, así como al progreso de las actuaciones del Mecanismo Único de Supervisión. Desde la perspectiva de las infraestructuras de mercado, el Banco de España participa en la vigilancia de los sistemas de pago de la zona del euro y de los depositarios centrales de valores, así como en los colegios de supervisores de las entidades de contrapartida central.

En el plano nacional, adicionalmente al ejercicio de sus responsabilidades supervisoras y de vigilancia, desarrolla numerosas actividades horizontales encaminadas a obtener un conocimiento global de la situación tecnológica de las entidades españolas y a mejorar la ciberseguridad y ciberresiliencia tanto de estas como del sector financiero en su conjunto.

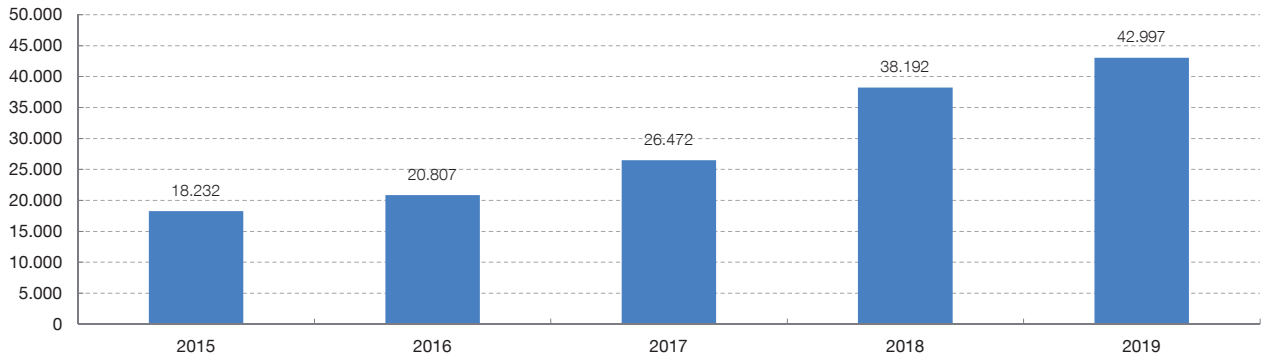
3.2 Situación actual

Tal y como se ha mencionado anteriormente, en los últimos años se han incrementado notablemente la frecuencia y la sofisticación de los ataques de los que ha sido víctima el sector financiero. En el gráfico 2 podemos ver el aumento del número de ciberincidentes ocurridos en España y gestionados por el Centro Criptológico

38 Véase Banco Central Europeo (2018).

39 Véase Comité de Supervisión Bancaria de Basilea (2018).

Gráfico 2
NÚMERO DE INCIDENTES GESTIONADOS POR EL CCN-CERT



FUENTE: Centro Criptológico Nacional (2020).

Nacional (CCN)[40], de los que un importante porcentaje tuvieron como objetivo el sector financiero. Los datos del CCN también muestran que un 64 % de los incidentes que gestionaron en 2019 fueron clasificados con una peligrosidad alta, muy alta o crítica[41].

Es difícil cuantificar con precisión los costes asociados a los ciberincidentes, puesto que, a pesar de que en los últimos años se han realizado numerosos estudios al respecto, todavía adolecemos de definiciones comunes y de datos históricos fiables, homogéneos y comparables. Sin embargo, hay unanimidad respecto a que el impacto negativo de los ciberincidentes, incluyendo las pérdidas económicas asociadas, se reduce en aquellas compañías que disponen de medidas adecuadas para proteger sus sistemas, detectar tempranamente los incidentes cuando ocurren y tener mecanismos de respuesta y recuperación frente a ellos.

La pandemia de COVID-19, muy prolongada en el tiempo y de ámbito global, ha resaltado el papel crucial de una adecuada gestión de las TIC y la importancia de la ciberresiliencia para el correcto funcionamiento del sector financiero. De hecho, pese al incremento en la exposición a los ciberincidentes y el aumento en el número de ciberataques recibidos, el impacto en el sector ha sido limitado. Es justo reconocer que ello se debe en buena medida a los esfuerzos e inversiones previos que tanto las autoridades como las infraestructuras de mercado, las entidades y sus proveedores, que se han convertido en una pieza clave del ecosistema, han realizado en los últimos años para mejorar su ciberresiliencia.

40 Véase Centro Criptológico Nacional (2021).

41 En el informe *Ciberamenazas y tendencias. Edición 2020* se clasifican los incidentes en cinco niveles de peligrosidad: crítico, muy alto, alto, medio y bajo.

Una de las áreas fundamentales para lograr este objetivo es la adecuada gestión de todos sus activos tecnológicos, desde los elementos de infraestructura hasta los datos, cubriendo su ciclo de vida completo: identificación, clasificación según su nivel de criticidad, realización de los cambios necesarios para mantener su vigencia de modo diligente y seguro, monitorización constante del estado del activo, y eliminación controlada cuando cesa su uso.

Además, como respuesta a un entorno en el que las ciberamenazas son cada vez más frecuentes y el nivel de sofisticación de los atacantes se incrementa, las entidades han evolucionado desde un enfoque centrado en la protección de sus conexiones con el exterior, o perímetro, hasta otro más holístico, en el que es fundamental tener en cuenta todos los posibles vectores de amenaza, incluyendo los internos. Así, mientras siguen trabajando en seguridad perimetral, incorporan como nuevo foco la segmentación de su red interna, esto es, la segregación de la red de una entidad en subredes estancas, mecanismo de seguridad fundamental ya que impide o dificulta que un atacante que comprometa un sistema tenga acceso a otros sistemas de la entidad fuera de la subred comprometida.

Como parte de ese enfoque holístico que va más allá de la tecnología y en el que el factor humano es fundamental, resulta crucial la formación y concienciación de todos los empleados de las entidades, incluyendo los de sus proveedores. Es necesario destacar la importancia de estas medidas, puesto que en muchas ocasiones los empleados son los vectores de entrada más utilizados por los atacantes, ya que constituyen el eslabón más débil de la cadena. En este sentido, las entidades vienen desarrollando en los últimos años programas formativos en materia de ciberseguridad, tanto para la dirección como para el resto de los empleados, que incluyen cursos y ejercicios prácticos, como simulación de ataques de *phishing* o *vishing*.

Como se ha explicado anteriormente, el concepto de *ciberresiliencia* implica la capacidad de anticipar, resistir, contener y recuperarse rápidamente ante ciberincidentes. Es importante, en consecuencia, 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 capacidades de detección, respuesta y recuperación cobran especial relevancia, lo que enlaza con la disciplina de continuidad de negocio.

Con el objetivo de garantizar los niveles de ciberresiliencia deseados, las entidades establecen y prueban sus planes de continuidad de negocio y contingencia tecnológica, que contemplan diversos escenarios adversos, incluido 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.

3.3 Tendencias

Los rápidos avances de la tecnología y la constante evolución de su uso en la provisión de servicios financieros dibujan un escenario en continuo movimiento, en el que las amenazas y su materialización en los distintos riesgos también son cambiantes. Esto obliga a todos los participantes en el sector financiero a un proceso de adaptación constante, en el que las medidas que hoy son eficaces para conseguir los niveles de resiliencia objetivo mañana pueden no ser suficientes.

Al margen de las medidas concretas y los controles asociados al campo de la ciberseguridad, las entidades deben plantearse el paradigma o el modelo de ciberseguridad bajo el que quieren integrar el funcionamiento de dichas medidas. En este sentido, agencias gubernamentales como la NSA[42] u organismos de referencia en el ámbito tecnológico como el NIST[43] se han pronunciado a favor de la incorporación de arquitecturas *Zero Trust,* modelo que parte de dos premisas expuestas con anterioridad en este artículo: asumir que los ciberincidentes, tarde o temprano, ocurrirán, y gestionar un perímetro cada vez más difuso.

Hasta hace unos años existía una frontera clara entre la entidad y el entorno externo, más sencilla de identificar y gestionar. Ahora, esa frontera se difumina debido a multitud de conexiones, necesarias para el acceso remoto de los empleados y proveedores, la implementación de políticas de *Bring Your Own Device*[44] o la externalización de procesos, por ejemplo a proveedores de servicios en la nube. Cada una de estas nuevas conexiones, así como los activos que se conectan a la red de la entidad, deben ser monitorizados y controlados.

El modelo *Zero Trust* aboga por eliminar el principio de confianza en todas las operaciones. Es decir, bajo esta arquitectura se pretende segregar cada activo informático (incluidos los datos), y aplicar los fundamentos de mínimo privilegio y denegación por defecto, de forma que se verifique siempre la identidad del usuario, en cada operación relevante y de forma explícita.

Así, del mismo modo que hemos destacado la relevancia de la segregación de redes, que dificulta que un ataque exitoso se extienda en la red interna de una entidad, generalizamos el concepto para segregar todos los activos relevantes y verificamos la identidad en cada operación que traspase alguno de los límites que hemos construido. Evidentemente, este modelo, cuando se generalice, elevará el perfil de seguridad de las entidades y reducirá el impacto de los ciberincidentes,

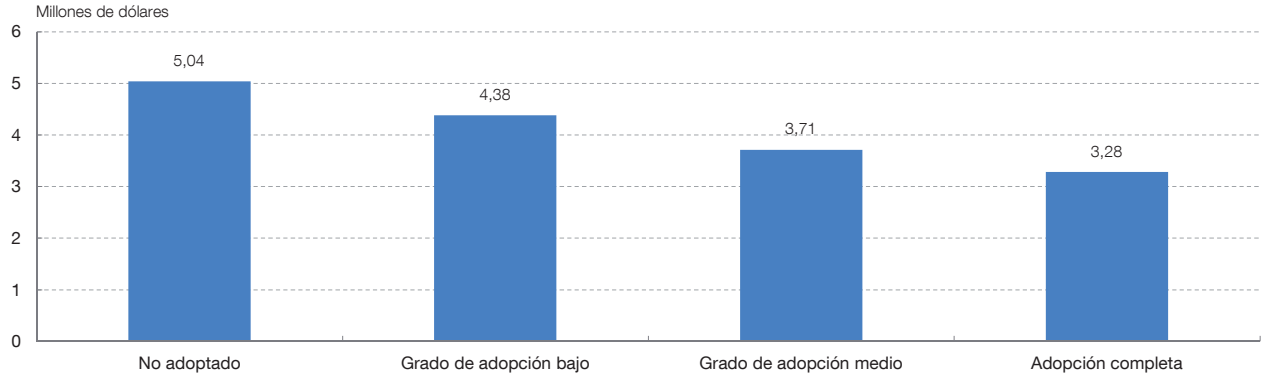
42 Véase NSA (2021).

43 Véase NIST (2020).

44 *Bring Your Own Device* («trae tu propio dispositivo», en inglés), abreviado con el acrónimo BYOD, es una política empresarial consistente en que los empleados lleven sus propios dispositivos personales (portátiles, tabletas, móviles) a su lugar de trabajo para tener acceso a recursos de la empresa tales como correos electrónicos, bases de datos y archivos en servidores, así como datos y aplicaciones personales.

Gráfico 3

COSTE MEDIO DE LA BRECHA DE DATOS EN FUNCIÓN DEL GRADO DE DESPLIEGUE *ZERO TRUST*



FUENTE: IBM-Ponemon (2021).

como podemos observar en el gráfico 3. Pero tiene desventajas, como el incremento de la complejidad y de la carga transaccional, o la reducción de la usabilidad, por lo que su implantación y su alcance requieren de un estudio detallado y basado en riesgos.

En cuanto a las nuevas tecnologías, la ciberresiliencia de las entidades financieras se verá particularmente afectada por la evolución de las tecnologías asociadas al campo de la Inteligencia Artificial. En este campo se identifican casos de uso en los ámbitos de la ciberseguridad ofensivos y defensivos, en lo que podría considerarse una carrera tecnológica.

En relación con la vertiente ofensiva, entre otros ejemplos, cabe subrayar el uso de soluciones de Inteligencia Artificial para burlar mecanismos de control de acceso tradicionales y, con mayor eficiencia aún, aquellos basados en imágenes o patrones de voz; embeber *malware*[45] en aplicaciones legítimas y controlar su ejecución, o lo que se ha denominado *smart malware,* es decir, *software* malicioso que aprende patrones de uso permitidos en una organización (ya sea de usuarios o programas), los emula, y utiliza las vulnerabilidades existentes para escapar a la detección y propagarse.

Por lo que se refiere a la vertiente defensiva, destaca el modelado del comportamiento del tráfico de red de una organización. La Inteligencia Artificial permitirá la detección de patrones anómalos especialmente complejos en volúmenes ingentes de información, más allá de lo que permiten las capacidades

45 Se llama *programa malicioso,* en inglés *malware,* cualquier tipo de *software* que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

de un analista humano o un sistema tradicional, y su integración con antivirus y sistemas de detección y prevención de intrusos.

El resultado de la carrera por explotar las posibilidades de la Inteligencia Artificial dependerá, en gran medida, de qué aplicaciones evolucionen más rápido y del ritmo de adopción de las entidades.

Las entidades continuarán fortaleciendo sus esquemas de recuperación, dado que, en último término y asumiendo la ocurrencia del ciberincidente, en determinadas circunstancias adversas necesitarán recuperar sus servicios ante una afectación de la integridad, la confidencialidad o la disponibilidad de su información. En dicho sentido, son especialmente interesantes las medidas de *data vaulting,* término que se refiere al almacenamiento fuera de línea *(offline)* y fuera de las instalaciones *(offsite)* del conjunto de datos críticos que precisa una entidad para mantener sus servicios críticos operativos.

Un ejemplo ilustrativo es la iniciativa que está llevando a cabo Sheltered Harbor, subsidiaria del Financial Services Information Sharing and Analysis Center (FS-ISAC), que cuenta con la participación y el apoyo de las principales asociaciones bancarias americanas[46]. El esquema de funcionamiento que han previsto implica que las entidades participantes envíen su información encriptada y en un formato acordado a instalaciones de data *vaulting* comunes, de modo que, en caso de contingencia mayor y en virtud de su participación en la iniciativa, sus datos puedan ser recuperados y procesados en las instalaciones de otras entidades participantes que no se hayan visto afectadas.

También las autoridades continúan redoblando sus esfuerzos en el ámbito de la resiliencia. Desde el punto de vista regulatorio, podemos destacar el desarrollo del *Digital Operational Resilience Act* (DORA), el nuevo reglamento de la Comisión Europea para el sector financiero. DORA se aplicará a todo tipo de entidades financieras, de cualquier tamaño, de modo proporcional, y contiene requerimientos sobre gestión de los riesgos asociados a la tecnología; identificación, clasificación y notificación a las autoridades de ciberincidentes relevantes; realización de pruebas de ciberresiliencia, y compartición de información. Pero DORA no solo unifica y eleva el nivel de exigencia en cuanto a cómo deben gestionar el ciberriesgo las entidades financieras, sino que establece un novedoso marco de vigilancia directa sobre los proveedores tecnológicos que sean considerados críticos para el sector financiero europeo. Este reglamento, cuya entrada en vigor se prevé para 2024, constituye una norma exigente y armonizada para todo tipo de entidades financieras, y sin duda contribuirá a mejorar la resiliencia del sector.

46 Véase sitio web de la iniciativa Sheltered Harbor.

Otro ámbito en el que están trabajando las autoridades de muchas jurisdicciones es fomentar que las entidades financieras e infraestructuras de mercado realicen pruebas de ciberseguridad estresadas, en las que se simulen ciberataques sofisticados. En ese sentido, el Banco de España está implementando TIBER-ES, la adopción local del marco de pruebas de ciberseguridad TIBER-EU, con el objetivo de mejorar el nivel de resiliencia del sector financiero español.

Además de que las entidades, individualmente, se sometan a estas pruebas, es importante promover también la realización de pruebas sectoriales, con el fin de mejorar los mecanismos de coordinación y comunicación en caso de eventos con impacto sistémico. Podemos destacar aquí los ejercicios del Cyber Expert Group del G-7, los trabajos del European Systemic Cyber Group (ESCG) o el mandato que DORA dará a las autoridades europeas del sector financiero para avanzar en esta dirección.

Cada vez resulta más evidente que, si hay un ámbito en el que la cooperación es clave, este es el de la ciberseguridad. Así lo han entendido las entidades, que comparten entre ellas información relevante sobre ciberincidentes y ciberamenazas (lo que se suele denominar «información de ciberinteligencia»), en diversos foros organizados por la industria, como por ejemplo FS-ISAC[47]. También existen ejemplos de cooperación entre entidades, autoridades y otros participantes del sistema financiero, como la plataforma CIISI-EU *(Cyber Information and Intelligence Sharing Initiative)*[48].

Asimismo, las autoridades están mejorando su cooperación, no solo dentro del sector financiero, sino incluso con otras autoridades transversales en materia de ciberseguridad, como los centros de respuesta ante ciberincidentes o las agencias de inteligencia.

El papel de las autoridades del sector financiero ha ido cambiando en paralelo al aumento de la importancia de la tecnología y del objetivo de mejorar la ciberresiliencia. Se ha pasado de un enfoque tradicionalmente centrado en la solvencia y la liquidez de las entidades y en el correcto funcionamiento de las funciones financieras críticas a considerar la tecnología como elemento indispensable para el funcionamiento del sector y a supervisar su uso y su evolución, así como la de los riesgos asociados. Más aún, las autoridades están adoptando un rol activo en el terreno de la ciberresiliencia, y se han convertido en una pieza clave en la gestión y la coordinación de posibles crisis derivadas de un ciberincidente.

No obstante, el papel central a la hora de mejorar la ciberresiliencia del sector financiero lo seguirán teniendo las entidades financieras, las infraestructuras de

47 Véase sitio web de FS-ISAC.

48 Véase sitio web de CIISI-EU.

mercado y los proveedores. Continuando su esfuerzo en este ámbito, deberán integrar la gestión del factor humano y organizativo con su propia evolución tecnológica, los avances en ciberseguridad y en continuidad de negocio, si quieren hacer frente con éxito al previsible aumento de la sofisticación y el impacto de los ciberataques.

BIBLIOGRAFÍA

Autoridad Bancaria Europea (2019). *Directrices de la ABE sobre gestión de riesgos de TIC y de seguridad,* noviembre.

Banco Central Europeo (2018). *Cyber resilience oversight expectations for financial market infrastructures,* diciembre.

Banco Central Europeo (2021). *Annual report on the outcome of the 2020 SREP IT Risk Questionnaire - Feedback to the industry,* julio.

Banco de Inglaterra (2018). *Building the UK financial sector's operational resilience,* documento de debate del Banco de Inglaterra y la Autoridad de Conducta Financiera (FCA, por sus siglas en inglés), julio.

Banco de Pagos Internacionales (2021). «Covid-19 and cyber risk in the financial sector», *BIS Bulletin,* n.º 37, enero.

Centro Criptológico Nacional (2020). *Ciberamenazas y tendencias. Edición 2020,* CCN-CERT IA-13/20, septiembre.

Comité de Supervisión Bancaria de Basilea (2011). *Principles for the Sound Management of Operational Risk,* junio.

Comité de Supervisión Bancaria de Basilea (2014). *Cyber resilience in financial market infrastructures,* noviembre.

Comité de Supervisión Bancaria de Basilea (2018). *Cyber-resilience: range of practices,* diciembre.

Comité de Supervisión Bancaria de Basilea (2021a). *Principles for Operational Resilience,* marzo.

Comité de Supervisión Bancaria de Basilea (2021b). *Revisions to the Principles for the Sound Management of Operational Risk,* marzo.

Consejo de Estabilidad Financiera (2018). *Cyber Lexicon,* 12 de noviembre.

Council on Foreign Relations (2021). *Cyber Operations Tracker,* base de datos pública de ciberincidentes patrocinados por Estados.

CPMI-IOSCO (2016). *Guidance on cyber resilience for financial market infrastructures,* junio.

Departamento de Seguridad Nacional (2017). *Estrategia de seguridad nacional*.

Departamento de Seguridad Nacional (2019). *Estrategia Nacional de Ciberseguridad*.

Departamento de Seguridad Nacional (2021). *Informe Anual de Seguridad Nacional 2020,* marzo.

Hernández de Cos, P. (2019). «Financial technology: the 150-year revolution», discurso pronunciado como presidente del BCBS en la *22.ª Euro Finance Week* de Fráncfort, de 19 de noviembre.

Herrera, F. J., J. Munera, y P. Williams (2021). «Cyber risk as a threat to financial stability», *Revista de Estabilidad Financiera,* n.º 40, primavera, Banco de España.

IBM-Ponemon (2021). *Cost of a Data Breach Report 2021*.

Junta Europea de Riesgo Sistémico (2020). *Systemic cyber risk,* informe del European Systemic Cyber Group, febrero.

Naciones Unidas (2019). *Final report of the Panel of Experts of the 1718 DPRK Sanctions Committee,* informe del Consejo de Seguridad referente a la República Popular Democrática de Corea, 5 de marzo.

NIST (2020). *Zero Trust Architecture,* NIST Special Publication 800-207, publicación de Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de Estados Unidos (NIST, por sus siglas en inglés), agosto.

NSA (2021). *Embracing a Zero Trust Security Model,* informe de ciberseguridad publicado por la Agencia de Seguridad Nacional de Estados Unidos (NSA, por sus siglas en inglés), febrero.

Unión Internacional de Telecomunicaciones (2021). *Global Cybersecurity Index 2020.*