BANCO DE ESPAÑA
Eurosistema

12.04.2024

El ciberriesgo y sus implicaciones para la estabilidad financiera

Punto de Encuentro Financiero FINANZA/Elkargi

Bilbao

Pablo Hernández de Cos
Gobernador

Señoras y señores, buenos días. Quiero empezar agradeciendo a Elkargi la organización de este encuentro y la oportunidad que me brindan de participar en él.

En esta ocasión querría compartir con ustedes unas reflexiones en torno al ciberriesgo[1] y sus implicaciones para la estabilidad financiera. La imparable digitalización de la economía y la sociedad lo han convertido en una prioridad para todos, y de modo particularmente significativo para el sector financiero y sus autoridades de supervisión y regulación.

La creciente digitalización del negocio bancario…

El sector financiero está fuertemente digitalizado. Las entidades dependen de la tecnología no solo como un elemento fundamental de apoyo al negocio, sino también como un factor diferencial y competitivo.

En los últimos años el proceso de transformación digital se ha acelerado, tanto para mejorar la eficiencia de los procesos internos de las entidades como para ofrecer a sus clientes servicios flexibles, personalizados y accesibles de forma inmediata, desde cualquier lugar y con distintos tipos de dispositivos.

La pandemia del COVID-19 y la aparición de nuevos competidores, como son las *bigtech* o las *fintech*, han reforzado estos desarrollos.

ha incrementado la exposición de las entidades financieras y sus clientes al ciberriesgo …

Este proceso de digitalización ha aumentado la exposición del sector financiero a los ciberriesgos. Del mismo modo, la ampliación de la oferta de servicios financieros a distancia ha aumentado la exposición de los clientes a ciberataques y fraudes digitales.

El número de ciberincidentes no ha parado de crecer en los últimos años, con un repunte especialmente relevante de los de naturaleza maliciosa[2], estando el sector financiero entre los más afectados[3]. Y no solo el número de ciberataques crece, también aumenta su sofisticación e impacto potencial, ya sea movidos por motivaciones estrictamente económicas o geopolíticas[4]. En particular, se ha observado un incremento de los ciberataques tras la invasión de Ucrania por Rusia.

[1] Se entiende por ciberriesgo la combinación de la probabilidad de ocurrencia de ciberincidentes con su impacto. Estos últimos los define el Financial Stability Board (FSB) en su Cyber Lexicon como aquellos eventos, tanto maliciosos como no maliciosos, que comprometen la confidencialidad, la integridad o la disponibilidad de la información o los sistemas de información interconectados.

[2] Los ciberriesgos incluyen aquellos provocados por desastres naturales, errores humanos o fallos accidentales en los sistemas. De hecho, los ciberincidentes no maliciosos son los más frecuentes, si bien, pese a su menor frecuencia, el impacto de los ciberataques suele ser mayor.

[3] El Centro Criptológico Nacional registró en 2023 107.777 ciberincidentes frente a los 42.997de 2019. Por su parte, el Informe de Seguridad Nacional de 2023, recientemente publicado, cita al sector financiero, junto con energía, TIC y transporte, como los que más volumen de ciberincidentes han registrado en los últimos años.

[4] Así, observamos ciberataques que buscan la realización de transferencias fraudulentas, 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)*.

Por tipología, se han registrado crecimientos muy significativos en aquellos casos de fraude que utilizan ingeniería social, como el *phishing*[5], el *smishing*[6] y el *vishing*[7], acompañados de suplantación de sitios web y aplicaciones móviles, entre otros.

Las pérdidas asociadas a los ciberincidentes son también significativas. Por ejemplo, las filtraciones de información - uno de los ciberataques cada vez más frecuente– supusieron un coste medio para las empresas de 4,45 millones de dólares en 2023 a nivel global. En el caso del sector financiero, además de presentar una mayor frecuencia, el coste medio de estas filtraciones fue también superior, 5,9 millones de dólares en 2023.

Además, hay que tener en cuenta que la capacidad de transferir este riesgo resulta limitada. Las pólizas de seguro para cubrirlo tienen un impacto mitigador reducido, ya que las coberturas financieras que ofrecen no suelen abarcar todos los efectos de un ciberincidente[8] y, además, las condiciones de estos seguros a escala global se han endurecido recientemente.

Y puede afectar a la estabilidad financiera

Las entidades financieras individualmente consideradas tienen entornos tecnológicos excepcionalmente 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. Esta complejidad supone un reto para las entidades a la hora de mantener un entorno de control adecuado y las hace más vulnerables, tanto a fallos en los sistemas como a ciberataques.

El sector financiero en su conjunto constituye un ecosistema también muy complejo, formado por numerosos participantes intensamente interconectados y dependientes entre sí. Y no hablamos solo de interconexiones financieras: existen también 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.

A las interconexiones tradicionales hay que sumar la aparición de nuevos actores que ofrecen servicios financieros y la creciente dependencia de los proveedores tecnológicos. En muchos casos, se produce una fuerte concentración en un número relativamente pequeño de estos proveedores, algo especialmente evidente en el caso particular de los relacionados con la computación en la nube. De hecho, algunos de estos proveedores

[5] Los ataques de *phishing* son aquellos en los que el 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.

[6] 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.

[7] 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.

8 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.

constituyen puntos únicos de fallo, de manera que los ciberincidentes que les afectan, incluso los no intencionados, pueden tener un impacto en el conjunto del sector y, por tanto, resultar sistémicos[9].

Como resultado, las autoridades macroprudenciales de distintas jurisdicciones, como es el caso de la Junta Europea de Riesgo Sistémico (JERS), incluyen al ciberriesgo entre las principales fuentes de riesgo sistémico en la actualidad[10].

Del ciberriesgo a la ciberresiliencia: hacia un enfoque holístico

Dado todo lo anterior, no es de extrañar que las implicaciones del ciberriesgo y las medidas para mitigarlo sean objeto de atención prioritaria tanto por las entidades financieras como por las autoridades prudenciales.

En este sentido, 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, y asumir que, a pesar de todos los esfuerzos preventivos, en algún momento se producirá un ciberincidente con impacto.

El concepto de ciberresiliencia surge precisamente como evolución del concepto de ciberseguridad, y se entiende 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[11].

A su vez, la ciberresiliencia se puede generalizar al concepto de resiliencia operacional, entendida como la capacidad de una entidad para mantener sus operaciones críticas en situaciones adversas[12].

Se trata, por tanto, de un enfoque 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 que enlaza con actividades más tradicionales, como la continuidad de negocio.

Las entidades están evolucionando hacia este enfoque holístico. Así, a la constante mejora de las medidas técnicas se ha añadido un significativo esfuerzo de formación y concienciación de sus empleados en materia de ciberseguridad, con el fin 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 las

[9] 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 serían escenarios con un potencial efecto sistémico.

[10] Véase, por ejemplo, *Systemic Cyber Risk*, ESRB 2020, (enlace).

[11] Véase el *Cyber Lexico*n del FSB.

[12] Véase los *Principles for Operational Resilience* del Comité de Supervisión Bancaria de Basilea.

funciones de gestión de riesgos y de auditoría en esta materia. Y, de igual manera, se esfuerzan en concienciar a sus clientes de la importancia de la ciberseguridad.

La necesaria respuesta regulatoria y supervisora

En cuanto a los reguladores y supervisores prudenciales, la respuesta está siendo amplia, tanto a escala global como europea y nacional, y tanto a nivel micro como macroprudencial. A escala global el Comité de Supervisión Bancaria de Basilea (BCBS) aprobó los Principios de Resiliencia Operacional en 2021, que establecen que los bancos deben asumir como hipótesis de trabajo que ocurrirán eventos adversos 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[13].

En la Unión Europea destaca el reglamento de resiliencia operativa digital, DORA por sus siglas en inglés, que tiene como objetivo mitigar los riesgos asociados a la digitalización y mejorar la resiliencia de todo el sector a través de:

- Requerimientos para todas las entidades financieras sobre la gestión de los riesgos asociados a la tecnología y a aquellos que se derivan de sus relaciones con terceros.

- La obligación de notificación a los supervisores de incidentes tecnológicos con el fin de detectar lo antes posible eventos adversos que pudieran requerir algún tipo de intervención por parte de las autoridades.

- La realización de pruebas sobre la resiliencia de los sistemas. Entre ellas, las más avanzadas consisten en simular ciberataques, 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.

En el ámbito de la supervisión microprudencial, las autoridades financieras del sector bancario europeo han incorporado el ciberriesgo como una de sus prioridades supervisoras, lo que se refleja en un refuerzo tanto del seguimiento continuo y las inspecciones *in situ* sobre las entidades como de las actividades horizontales centradas en este riesgo.

Para ello, han incrementado su dotación de recursos especializados y han establecido metodologías y procedimientos de trabajo adaptados a las particularidades de este riesgo. Así, el Mecanismo Único de Supervisión está llevando a cabo unas pruebas de resistencia frente a este riesgo en 2024.

Por su parte, la Junta Europea de Riesgo Sistémico (JERS) creó en 2017 un grupo de trabajo específico para el estudio del potencial impacto del ciberriesgo en la estabilidad financiera,

[13] Estos principios cubren aspectos de (i) gobernanza, (ii) gestión de riesgos operacionales, (iii) identificación continua de amenazas y de interconexiones e interdependencias, (iv) gestión de terceros, (v) continuidad de negocio y (vi) gestión de incidentes y de la tecnología, incluyendo la ciberseguridad.

el European Systemic Cyber Group (ESCG). Los diferentes análisis que se han realizado muestran:

- La utilidad de trabajar en escenarios de pruebas de ciberresiliencia a nivel sistémico[14].

- La necesidad de disponer de planes de respuesta ante ciberincidentes sistémicos y de someterlos a revisiones y pruebas periódicas.

- La deseabilidad de identificar las circunstancias en las que se puede desencadenar una crisis sistémica y establecer umbrales que permitan reaccionar y tratar de mitigar los impactos antes de que desemboque (lo que se conoce como *Systemic Impact Tolerance Objectives,* SITO)[15].

- La necesidad de crear un marco paneuropeo de coordinación en caso de ciberincidentes sistémicos que cubra las lagunas actuales.

Por su parte, con esta perspectiva sistémica, el reglamento DORA fomenta el intercambio de información entre instituciones y establece mecanismos de cooperación entre autoridades dentro y fuera del sector financiero. También 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 sector financiero europeo.

Herramientas macroprudenciales para la gestión del ciberriesgo: del capital financiero al capital tecnológico

En paralelo, se ha iniciado una discusión sobre los instrumentos más adecuados para mitigar los ciberriesgos.

En particular, se ha analizado el papel del capital prudencial. En este caso, se entiende que, en el escenario de una entidad afectada, por ejemplo, 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 no sería, por tanto, el principal elemento de resiliencia en este caso.

No obstante, más allá de que una mayor solvencia puede facilitar la financiación de las opciones requeridas para la recuperación de un ciberincidente, las potenciales consecuencias disruptivas para el conjunto del sistema financiero podrían, en ocasiones, 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. Por ejemplo, el uso del colchón contra riesgos sistémicos podría permitir discriminar entre entidades bancarias en función de su grado de sistemicidad tecnológica.

[14] También el reglamento DORA anima a las autoridades a organizar ejercicios de gestión de crisis y contingencia que incluyan escenarios de ciberataques, con el objetivo de hacer posible, gradualmente, una respuesta coordinada eficaz a escala de la Unión Europea.

[15] Para una función económica determinada, un SITO podría estar definido en virtud del número de operaciones impactadas, su valor en euros, la duración del ciberincidente o el número de entidades y jurisdicciones afectadas.

Todo ello podría contribuir a limitar la ocurrencia de eventos sistémicos y consiguientes fenómenos de contagio.

La materialización de ciberincidentes con un impacto financiero notable puede exigir también el despliegue de instrumentos financieros para la gestión de crisis e incluso el desarrollo de otros nuevos. Así, un ciberincidente podría provocar que una entidad viese limitada su operativa, causándole 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 tener sobre la estabilidad financiera y permitiendo continuar con la prestación del servicio a la economía.

En el mismo sentido, 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.

En todo caso, es probable que la resiliencia frente a ciberriesgos que puede aportar una cierta cantidad de capital puede alcanzarse de forma más eficaz y eficiente mediante la acumulación de recursos tecnológicos (*software*, *hardware*, conocimientos, personal especializado, etc.) que reduzcan la probabilidad de ocurrencia y el impacto financiero de los ciberincidentes. Por ejemplo:

- La introducción de *circuit-breakers*, que suponen la interrupción de procesos en crisis tecnológicas y financieras simultaneas, que limiten su contagio.

- El recurso a mecanismos colectivos de apoyo entre las entidades que permitan al sistema en su conjunto compartir capital tecnológico, haciendo así posible la reconducción colaborativa de procesos entre entidades en caso de fallo de una o, similarmente, el acceso a datos comprometidos en un ciberataque individual. En particular, 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*, participado y apoyado por las principales asociaciones bancarias americanas. Las entidades participantes envían su información encriptada y en un formato acordado a instalaciones comunes, de modo que sus datos puedan ser recuperados y procesados en una plataforma de recuperación.

Perspectivas futuras: la inteligencia artificial y la computación cuántica

Las posibilidades que ofrecen las nuevas tecnologías brindarán nuevas oportunidades a los defensores, pero también a los atacantes.

En el caso de la inteligencia artificial (IA), las capacidades de generación de contenidos facilitarán la suplantación de identidades y harán mucho más creíbles los ataques de ingeniería social. Asimismo, la IA puede ayudar a la creación de *malware* o a la optimización de los ataques.

En sentido contrario, la IA puede permitir a las entidades 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 puede facilitar automatizar parcialmente la respuesta, complementando así la labor de los analistas y acortando sustancialmente los tiempos de reacción.

Por su parte, se estima que la computación cuántica podría permitir la vulneración a medio plazo de una gran parte de los sistemas de cifrado actuales, afectando tanto a la confidencialidad como a la integridad de la información cifrada. 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.

No obstante, se está trabajando ya en la creación de algoritmos criptográficos 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.

Conclusiones

En resumen, aunque algunos estudios sugieren que el financiero es uno de los sectores clave mejor preparados frente a los ciberriesgos, en parte debido a su elevado grado de regulación y supervisión, la aceleración del proceso de digitalización, el desarrollo de nuevas tecnologías, el carácter sistémico del sector y la complejidad y dinamismo del riesgo tecnológico, hacen que esta deba mantenerse como un área de atención prioritaria en los próximos años, e incluso intensificar los esfuerzos recientes.

Esta adaptación requerirá incorporar a las organizaciones los perfiles técnicos necesarios, por lo que la captación y retención del talento seguirá siendo un reto para el sector y para las autoridades.

El intercambio de información sobre ciberamenazas y ciberincidentes será también crucial para mejorar las capacidades colectivas de defensa. En este sentido, la posición central de las autoridades, que bajo DORA recibirán notificaciones de ciberincidentes de las entidades, les permitirá devolver al sector información de utilidad.

Del mismo modo, la realización de pruebas de ciberresiliencia y ejercicios de gestión de crisis sectoriales, que incluyan la participación de los proveedores relevantes y de otros sectores respecto a los que existen interdependencias operativas, será fundamental en los próximos años.

Asimismo, es necesario seguir avanzando en la cuantificación y comprensión de los ciberriesgos para la estabilidad financiera y el potencial rol de las políticas macroprudenciales en su mitigación.