BANCO DE ESPAÑA
Eurosistema

22.11.2018

Discurso de clausura

XI Jornada de Tesorería y Riesgos/Cecabank

Juan Ayuso Huertas
Director general de Mercados, Operaciones y Sistemas de Pago

Permítanme antes de nada agradecer a Cecabank su invitación para clausurar esta Jornada. Es un placer estar hoy aquí con ustedes.

Con carácter general, los actos de clausura deben ser breves y centrarse en temas poco conflictivos. Basta con repasar el contenido de la agenda de esta XI Jornada de Tesorería y Riesgos para llegar a la conclusión de que esta no es la ocasión para hacer una excepción a esa regla. Por la variedad y el alcance de los temas tratados, estoy seguro de que han tenido una mañana vibrante, pero también agotadora. Voy por lo tanto a ser breve y voy tratar un tema en el que estoy convencido de que todos vamos a estar bastante de acuerdo: la creciente importancia de la ciber-seguridad en los mercados financieros.

Desde finales de los años ochenta asistimos a avances espectaculares en el terreno de la tecnología, que están provocando cambios importantes en muchas facetas de nuestras vidas. En el campo concreto de las finanzas, un resultado notable es que las transacciones financieras prácticamente han dejado de estar sujetas a restricciones de tiempo o de espacio. Cualquiera de nosotros puede hoy realizar casi cualquier operación financiera, cualquier día, a cualquier hora y con una contraparte radicada en casi cualquier lugar del mundo. En algún caso, incluso, esa transacción puede tener lugar y ser firme de manera prácticamente instantánea.

Los avances en la velocidad de computación, en la capacidad de almacenamiento de la información y en la rapidez con la que es posible gestionarla y diseminarla han acelerado el ritmo de la innovación financiera, un ritmo que, por otra parte, no era precisamente lento. En apenas unos años hemos asistido no solo a la proliferación de nuevos y atractivos términos como “la nube”, el “big data” o la “inteligencia artificial”, sino también al desarrollo de nuevos productos y servicios financieros, y a la aparición de nuevos proveedores de estos productos y servicios, que están modificando de una manera sustantiva el ecosistema financiero.

Desde el Banco de España seguimos con mucha atención este proceso, como lo prueba la reciente creación (en febrero de este mismo año) de la Dirección General Adjunta de Innovación Financiera e Infraestructuras de Mercado. Lo hacemos, por un lado, porque estamos interesados en contribuir, en la medida de nuestras posibilidades, a su desarrollo. Y lo hacemos también, como corresponde a nuestro papel, porque estos procesos de innovación inciden igualmente sobre el mapa de riesgos y de vulnerabilidades del sistema financiero. En esta intervención temo que voy a adoptar esta última perspectiva, la del vigilante del sistema, que es bastante menos agradecida que la primera, pero igualmente necesaria, si no más.

El paso a unas finanzas más digitalizadas ofrece grandes oportunidades para aumentar la eficiencia de los mercados y el nivel de bienestar y de satisfacción de los consumidores financieros. Al mismo tiempo, sin embargo, aumenta la exposición a las amenazas cibernéticas. En estos momentos, me atrevería a decir que la pregunta verdaderamente relevante no es tanto si una entidad ha recibido o no algún tipo de ataque cibernético, sino cuántos han sido estos y cuál ha sido su intensidad. Desafortunadamente, disponemos ya de suficiente evidencia para afirmar que el uso malicioso de las tecnologías de la información y la comunicación es uno de los principales riesgos para el buen funcionamiento de los mercados financieros y, por extensión, para la estabilidad financiera de las economías.

La responsabilidad última de enfrentar estos riesgos corresponde, como es habitual, a los propios participantes en estos mercados. Pero corresponde a las autoridades desarrollar el marco regulador y supervisor en el que deben diseñarse y aplicarse las medidas encaminadas a paliar esos riesgos. Dedicaré el resto de mi intervención a comentar brevemente cuánto y cómo hemos avanzando en este terreno, particularmente en el caso del Eurosistema.

La motivación última de los delincuentes cibernéticos para atacar a un determinado proveedor de productos o servicios financieros no es, seguramente, muy distinta de la de otros tipos de delincuente y se podría condensar, a grandes rasgos, en motivos económicos o ideológicos. Lo que sí es una característica singular de este tipo de delincuencia es que opera sobre un sector caracterizado por unos niveles sin igual de interconexión e interdependencia entre sus componentes. A estos efectos, el sector financiero es un sistema global y esto tiene dos implicaciones relevantes.

La primera es que, ya sea en términos económicos o en términos de "altavoz ideológico", el potencial beneficio de un ataque cibernético eventualmente exitoso es muy elevado. La segunda, es que la ciber-seguridad ha de afrontarse desde una perspectiva global, que interiorice en su construcción ese elevado grado de interconexión entre todos los componentes del sistema.

En este contexto, en junio de 2016 y sobre la base de iniciativas previas adoptadas al nivel del G7, CPMI --el Comité de Pagos e Infraestructuras de Mercado del BIS-- e IOSCO --la Organización Internacional de Comisiones de Valores-- publicaron conjuntamente la "Guía sobre ciber-resiliencia cibernética para las infraestructuras de los mercados financieros".

Permítanme un inciso. Hasta ahora he utilizado el término ciber-seguridad. La Guía sin embargo utiliza el término ciber-resiliencia. La diferencia no es un simple matiz semántico. Antes al contrario, revela que la estrategia de mitigación de los riesgos cibernéticos no puede centrarse exclusivamente en la capacidad de defensa frente a los ataques. El nuevo enfoque que se adopta en esta Guía incide en la necesidad considerar seriamente la posibilidad de que en algún momento se produzca un ataque exitoso y requiere por tanto a las infraestructuras capacidad para detectar con prontitud ese tipo de incidente y para responder rápidamente al mismo, minimizando así el alcance de los daños.

La Guía establece cinco categorías principales en torno a las cuales diseñar la gestión de los riesgos cibernéticos. Concretamente: gobernanza, identificación, protección, detección, y respuesta y recuperación. Son precisamente las dos últimas categorías –la detección y la capacidad de respuesta y recuperación— las que marcan la diferencia entre la ciber-resistencia y la ciber-resiliencia.

La Guía establece también tres componentes generales sobre los que articular las estrategias de defensa en cada una de las categorías: la realización de pruebas de resistencia/resiliencia, el conocimiento de las amenazas existentes y de su posible impacto sobre las entidades, y el aprendizaje y la evolución.

Como corresponde a una guía de esta naturaleza, la Guía CPMI-IOSCO establece principios generales que las autoridades reguladoras y supervisoras deben posteriormente desarrollar. En este sentido, en marzo de 2017, el Consejo de Gobierno del BCE aprobó la

Estrategia de Resiliencia Cibernética del Eurosistema para las Infraestructuras de los Mercados Financieros bajo su competencia.

La Estrategia diseñada por el BCE se estructura en torno a tres pilares. El primero se centra en las infraestructuras de los mercados financieros y su objetivo es garantizar que se encuentren adecuadamente preparadas para hacer frente a las amenazas cibernéticas. El segundo pilar amplía el perímetro de actuación y fija como objetivo fortalecer la resiliencia del sector financiero en su conjunto. Por último, el tercer pilar busca promover el diálogo estratégico entre la industria y los reguladores con objeto de catalizar iniciativas conjuntas y desarrollar soluciones efectivas.

Los tres pilares, que están estrechamente interrelacionados, tienen asociada una serie de herramientas útiles para alcanzar los objetivos previstos.

La primera herramienta del pilar 1 es la llamada Encuesta Cibernética. Esta Encuesta se ha enviado por primera vez a todas las infraestructuras del mercado financiero en el Eurosistema para conocer su grado de madurez en términos de resiliencia cibernética e identificar aquellas áreas donde es necesario realizar un mayor esfuerzo de mejora.

Un segundo instrumento desarrollado por el Eurosistema en el contexto también de este primer pilar es un marco concreto para la realización de pruebas de penetración de tipo *red teaming,* que se ha bautizado como TIBER. Las pruebas de *red teaming* están inspiradas en experimentos similares en el terreno de la defensa militar y, en definitiva, consisten en replicar con el mayor realismo posible un ciber-ataque para probar las capacidades de detección, defensa y recuperación de las infraestructuras del mercado. El marco TIBER establece una serie de elementos obligatorios para el desarrollo de este tipo de pruebas, lo que permite asegurar unos estándares comunes de calidad que, a su vez, deberían sustentar el reconocimiento mutuo de este tipo de pruebas en toda la Unión Europea.

Para completar el conjunto de herramientas de este primer pilar hay que señalar también que el Eurosistema ha elaborado las Expectativas de Resiliencia Cibernética (CROE, por sus siglas en inglés) para los sistemas de pago. Estas Expectativas proveen a las infraestructuras de pagos y a las autoridades responsables de su vigilancia una referencia más concreta para la implementación y cumplimiento con las orientaciones generales establecidas en la Guía CPMI-IOSCO.

Pasando ahora al segundo pilar, el énfasis se pone en este caso en el intercambio de información y en la correcta comprensión de las interdependencias entre las distintas infraestructuras del mercado financiero. Con este objetivo, se está trabajando en la elaboración de un mapa de interdependencias que permitirá identificar los nodos críticos del ecosistema.

Un elemento fundamental en este segundo pilar es el intercambio eficiente de información entre los participantes del mercado, entre éstos y los reguladores, y entre los reguladores mismos. En el ámbito de la vigilancia y de la supervisión existen ya protocolos para la comunicación de incidentes, incluidos los incidentes cibernéticos. Pero es necesario un cambio de mentalidad que permita ir más allá de la mera notificación y marcar como objetivo el intercambio de inteligencia operativa, táctica y estratégica, incluso ex ante. Más tarde volveré sobre este asunto.

Antes, sin embargo, completaré la revisión de las herramientas contempladas en la Estrategia del Eurosistema señalando que para el buen desarrollo del tercero de los pilares se ha creado un nuevo foro, cuya primera reunión tuvo lugar el pasado 9 de marzo de este mismo año. Se trata del Consejo de Ciber-resiliencia del Euro para las Infraestructuras Financieras Paneuropeas. Su objetivo es promover la confianza y la colaboración entre los principales actores en este ámbito y catalizar iniciativas conjuntas para reforzar la resiliencia del sector. La lista de los Miembros iniciales de este foro incluye a los representantes de las principales infraestructuras y proveedores de servicios críticos del área del euro. Adicionalmente, asisten a las reuniones representantes de 7 Bancos Centrales Nacionales del Eurosistema, el Banco de España entre ellos; 3, de bancos centrales de la UE pero no pertenecientes al Eurosistema; y uno del propio BCE. A los representantes de los bancos centrales se les asigna un rol, el de Participante Activo, que es distinto del rol de Miembro. La lista de asistentes se completa con un conjunto relativamente amplio de instituciones como la Comisión Europea o Europol, entre otras, cuyos representantes asisten en el papel de observadores. El mandato de este Consejo es público y puede consultarse en la página web del BCE.

En definitiva, la Estrategia del Eurosistema es bastante ambiciosa y constituye sin duda un paso necesario para mitigar los riesgos para la estabilidad financiera que se derivan de la sofisticación, la frecuencia y la persistencia de los ataques cibernéticos.

Pero la colaboración decidida del Eurosistema, en particular, y de los supervisores y reguladores, en general, no es suficiente. La resiliencia cibernética del sistema financiero requiere un esfuerzo colectivo, en el que las entidades privadas que configuran el ecosistema financiero tienen un papel central. Este esfuerzo pasa por el adecuado conocimiento de las responsabilidades propias y debe descansar en una colaboración muy estrecha entre todos los afectados. Y vuelvo en este punto al tema del cambio en la mentalidad con la que el sistema financiero ha afrontado hasta ahora otros problemas de gestión de riesgos.

Es bien sabido que la fortaleza de una cadena la determina su eslabón más débil. Frente al riesgo de crédito, por utilizar quizá el ejemplo más “clásico” de riesgo, cabe pensar en el conjunto del sistema financiero como la suma de varias cadenas que, a su vez, están más o menos interconectadas entre sí. En ese caso, es razonable dedicar especial atención a los nodos que unen las cadenas. Para ser un poco más técnico: a los *big players* sistémicos.

Frente al riesgo cibernético, sin embargo, el sistema financiero se asemeja más a una cadena única. En este caso, los eslabones “pequeños” cuentan igual que los eslabones “grandes” a la hora de determinar si la cadena en su conjunto resistirá o no la tensión.

Por lo tanto, la noción de resiliencia cibernética hay que introducirla en el día a día de todas --y subrayo el todas-- las entidades. El principio de proporcionalidad, que puede tener sentido en otros contextos, es menos justificable en este caso.

Y creo que hay un segundo cambio importante: Convertirse en el alumno aventajado de la clase de ciber-resiliencia puede servir de poco si los progresos realizados no vienen acompañados de una creciente disposición a compartirlos plena y abiertamente con el resto de los compañeros de curso. Volviendo al símil de la cadena, cuando esta se rompe, no creo que sirva de mucho consuelo argumentar que uno era el eslabón más fuerte de esa cadena que, al fin y al cabo, se rompió y dejó de ser útil.

Es cierto que encontrar el equilibrio entre colaboración y competencia ha sido siempre un reto para el sector financiero. El peligro es que se infravalore el hecho de que los avances tecnológicos están modificando de manera muy sustantiva el terreno de juego en el que debe determinarse ese equilibrio.

Enfrentados al reto de la ciber-resiliencia, me parece importante, y con esto concluyo, que todos los implicados hagamos también un esfuerzo para huir de aproximaciones demasiado estrechas o demasiado tradicionales y adoptemos por el contrario nuevas perspectivas suficientemente amplias. Creo que frente a una amenaza que es global, la estrategia con mayor probabilidad de éxito es la que hace de la colaboración su principal herramienta.

Muchas gracias por su tiempo y por su atención.