Presentación del "Proyecto Resiliencia operativa digital en la gestión de activos: Más digitales, más seguros" (DORA) /INVERCO

VÍCTOR RODRÍGUEZ QUEJIDO, DIRECTOR GENERAL DE POLÍTICA ESTRATÉGICA Y ASUNTOS INTERNACIONALES DE LA CNMV

9 de mayo de 2023

Buenos días,

Es obvio que la tecnología ha ido adquiriendo una relevancia creciente en nuestras vidas y de que forma parte, cada vez más, de todos los servicios y productos que consumimos en el día a día, de cómo nos relacionamos y trabajamos. Y, sin duda, el sector financiero es uno de los ámbitos tradicionalmente más intensivos en el uso de tecnología.

Esta creciente dependencia digital, si bien implica beneficios claros en términos de eficiencia, también conlleva riesgos que hay que gestionar adecuadamente y uno de los más relevantes, que es el que precisamente se va a tratar aquí hoy, es el de la ciberseguridad en las entidades financieras.

La ciberseguridad lleva tiempo siendo un componente esencial a tener en cuenta pero se está haciendo aún más relevante porque estamos viviendo unos años de continua y exponencial innovación tecnológica. La inteligencia artificial, las tecnologías de registro distribuido o la computación cuántica son ejemplos de tecnologías que están teniendo un gran desarrollo en los últimos años y que generan importantes y adicionales retos en materia de ciberseguridad.

Precisamente el Reglamento sobre la resiliencia operativa digital (conocido como Reglamento DORA), consciente el legislador al elaborarlo del riesgo cada vez mayor de ciberataques, lo que pretende es reforzar la seguridad informática de las entidades financieras. Para ello establece unos requisitos uniformes para la seguridad de las redes y sistemas de información de estas entidades, así como para terceros que les presten servicios esenciales relacionados con las TIC (tecnologías de la información y la comunicación), como plataformas en la nube o servicios de análisis de datos. El Reglamento DORA crea un marco regulador conforme al cual todas las empresas deben asegurarse de que pueden resistir y responder a cualquier tipo de perturbación y amenaza relacionada con las TIC y recuperarse del potencial impacto derivado de ellas.

No voy a entrar en los detalles de esta nueva norma pero hay varias circunstancias relacionadas con la ciberseguridad que me gustaría resaltar.

En primer lugar, el aumento de los ataques, año tras año, y no sólo en número, sino también en tipología, persistencia y complejidad. Y esto es así porque los atacantes son cada vez más sofisticados, más profesionales, con mayores recursos, que además persiguen en muchas ocasiones objetivos geopolíticos o financieros, siendo por tanto las entidades financieras unas de sus víctimas favoritas.

En segundo lugar, el sistema financiero está cada vez más interconectado y es cada vez más global, lo que claramente aumenta el riesgo de contagio en un entorno altamente digitalizado, lo cual podría llegar a tener carácter sistémico, algo que, obviamente, es deseable evitar.

Por último, se ha producido un incremento en la contratación de servicios tecnológicos externos debido a diversos factores como los grandes volúmenes de datos o la necesidad de alta especialización. Lo cual puede generar dos potenciales situaciones críticas relacionadas con la ciberseguridad. La primera, una mayor exposición a amenazas a lo largo de toda la cadena de valor, ya que se incrementa la exposición de ataque al añadir diversos proveedores tecnológicos. Para gestionar este riesgo, los contratos deben incluir, de forma rigurosa, las obligaciones del proveedor en materia de ciberseguridad. Las directrices sobre la externalización de servicios a proveedores de servicios en la nube, publicadas por ESMA en mayo de 2021, establecen ya de forma clara el procedimiento adecuado para gestionar la contratación de ese tipo de servicios, y DORA incorpora un capítulo completo en el que introduce los requerimientos que las entidades financieras deberán cumplir en este ámbito. Surge también otro posible escenario en el que un proveedor de servicios tecnológicos que provea de servicios a una parte importante del sector financiero, sufra un ataque severo, afectando a los servicios que ofrece a un número elevado de entidades financieras, lo que implicaría un escenario grave para el sector. DORA también contempla este riesgo y establece procedimientos para la identificación de estos proveedores críticos y su supervisión desde órganos creados específicamente para supervisarlos desde una perspectiva global europea. Sin duda, va a ser un reto importante que tendremos que abordar entre todos.

Hacía referencia hace un momento a la complejidad de los nuevos ataques. Las amenazas persistentes avanzadas, conocidas como APTs por sus siglas en inglés, son probablemente el mayor reto al que nos tenemos que enfrentar en estos momentos. Los atacantes recopilan información sobre su objetivo, lo que se conoce como labores de inteligencia, durante el tiempo necesario hasta poder configurar un ataque más eficaz, contando cada vez con mayores recursos, y siendo por tanto más peligroso. Para estar preparadas ante estos ataques persistentes, las entidades financieras deberán llevar a cabo tests específicos para este tipo de amenazas. No se trata, por tanto, de someterse a los habituales tests de penetración, sino a tests que prueben los sistemas críticos frente a las APTs. No es nada nuevo, se llevan haciendo estas pruebas avanzadas desde hace años, y DORA lo exigirá únicamente para determinadas entidades financieras. Lo que sí es más reciente es la adopción del marco europeo de pruebas TIBER-EU, que viene a estandarizar estas pruebas entre las diferentes jurisdicciones que las adoptan. En el caso

de España, la adaptación de este marco se denomina TIBER-ES, y podrán someterse a pruebas bajo el mismo las entidades financieras que lo deseen, siempre que tengan el grado de madurez necesario en materia de ciberseguridad, ya que no hay que olvidar que estas pruebas se realizan contra los sistemas en producción.

Un aspecto sobre DORA que somos conscientes que preocupa al sector aunque también a los propios supervisores, es todo lo relativo a la proporcionalidad en la aplicación de la norma. DORA recoge en su propio articulado mecanismos de proporcionalidad.

Así, se ha incorporado un artículo (art.4) que establece el principio general de proporcionalidad que debe regir la aplicación y el cumplimiento del Reglamento por parte de las entidades financieras, teniendo en consideración aspectos tales como su tamaño y perfil de riesgo, así como la naturaleza, escalabilidad y complejidad de sus servicios, actividades y operaciones. Los supervisores deberemos aplicar este principio de forma sensata, de forma que exista un equilibrio entre la adecuada gestión del riesgo tecnológico y el esfuerzo que deberán realizar las entidades financieras.

Por poner un ejemplo, se establecen excepciones del cumplimiento de determinados requisitos para las microempresas (menos de 10 empleados y volumen de negocio o balance anual menor de 2 millones de euros), que son una gran parte de las empresas de servicios de inversión y las gestoras de nuestro país. De igual forma, se excluye de la aplicación de un número relevante de obligaciones a las empresas de inversión "pequeñas y no interconectadas", y se detallan obligaciones concretas alternativas más acordes a los recursos de este tipo de entidades.

Por otro lado, se incluyen obligaciones adicionales para las cámaras centrales de contrapartida, los depositarios centrales de valores y los proveedores de datos, dado su papel frecuentemente clave dentro del sistema.

Termino con un último mensaje que creo relevante. En la CNMV somos conscientes del reto que supone esta nueva normativa para todos. Por ello tenemos previsto realizar actuaciones de formación a nivel interno para nuestros técnicos y también hemos recogido en nuestro plan de actividades para 2023 el objetivo de hacer una evaluación del grado de preparación para DORA de las ESI y gestoras, de cara a planificar la entrada en aplicación de este Reglamento que, como es conocido, se producirá en enero de 2025. Para ello, durante este año vamos a elaborar un cuestionario dirigido a las ESI y gestoras relativo a los aspectos de ciberseguridad que se recogen en esta norma para poder analizar los resultados y tener una idea de cómo estamos en estas cuestiones. Nuestra intención es acompañar al sector en la implementación de DORA, mantener un diálogo permanente en este ámbito y trabajar conjuntamente para, entre todos, conseguir un sistema financiero más seguro y resiliente.

Muchas gracias