Recuadro 2.4

LA IMPORTANCIA DE LA GESTIÓN DEL RIESGO DE LOS PROVEEDORES TECNOLÓGICOS EN EL SECTOR FINANCIERO

Es un hecho contrastado que las entidades financieras de todo el mundo se apoyan en proveedores externos para la prestación de sus servicios. Los acuerdos con estas terceras partes, en muchas ocasiones, son complejos y pueden implicar a distintos proveedores localizados en diferentes jurisdicciones. Esta tendencia se incrementó por la pandemia de COVID-19, que obligó a las entidades a adoptar rápidamente servicios tecnológicos proporcionados por terceros para poder continuar ofreciendo sus servicios a los clientes. Este hecho incrementó su superficie de exposición y, por tanto, el riesgo operacional al que se enfrentan las entidades.

Por otro lado, es habitual que los proveedores externos de servicios tecnológicos presten sus servicios mediante una cadena de externalización, en la que en cada eslabón es un tercero distinto el que proporciona una parte del servicio. La complejidad de estas cadenas de proveedores dificulta la gestión y reduce la capacidad de mitigación de los riesgos, tanto de las entidades como de las autoridades supervisoras o de resolución, pues es extremadamente difícil identificar a todos los participantes involucrados y, por tanto, muy complejo evaluar adecuadamente el impacto que podría tener un incidente o la disrupción del servicio prestado por uno de ellos, no solo en una entidad particular, sino en el sector financiero en su conjunto.

Preocupadas por estos riesgos, en los últimos años las distintas autoridades europeas han emitido normativa para mitigar el riesgo de las externalizaciones —directrices EBA/GL/2019/02, sobre externalización de la Autoridad Bancaria Europea (EBA, por sus siglas en inglés), y circulares del Banco de España 2/2016 y 3/2022, entre otras—, que tanto las entidades como los proveedores han ido incorporando en sus acuerdos. Dada su relevancia para que las entidades puedan gestionar adecuadamente los riesgos, ambas normas establecen diversos requisitos para los contratos de externalización, especialmente para los que se refieren a servicios o funciones esenciales, como que incluyan cláusulas de derecho de acceso y auditoría para la entidad y para el supervisor o de terminación y salida. Consecuentemente, la evaluación de estos acuerdos sobre servicios o funciones esenciales se ha incorporado a la supervisión microprudencial de las entidades.

No obstante, las autoridades supervisoras y los organismos reguladores consideran que es necesario ampliar el alcance normativo e incluir en él todas las relaciones con terceros y, en particular, centrarse en la vigilancia de los proveedores de servicios críticos para el sector financiero. Muestra de ello son las iniciativas de las Autoridades Europeas de Supervisión —EBA, Autoridad Europea de Valores y Mercados y Autoridad Europea de Seguros y Pensiones de Jubilación— para recopilar los registros de los terceros tecnológicos, o la consulta pública del Consejo de Estabilidad Financiera sobre cuestiones relativas a la externalización de servicios y las relaciones con terceros, donde, entre otros aspectos, se destaca la necesidad de establecer una terminología común *(lexicon)* con definiciones globales y consistentes.

Adicionalmente, la próxima aplicación del Reglamento DORA *(Digital Operational Resilience Act)* establecerá requerimientos adicionales para las entidades y un marco de vigilancia de proveedores tecnológicos críticos para todo el sector financiero europeo.

Y ¿por qué tanta preocupación por el riesgo que puedan generar estos proveedores externos de servicios tecnológicos? La respuesta es inmediata, a los riesgos que lleva aparejada esta dependencia se añade la amenaza que representan los ataques a la cadena de suministro, que han proliferado en los últimos años, normalmente dirigidos a proveedores y desarrolladores de *software,* con el objetivo de alcanzar a una empresa a través de sus relaciones con terceros. El número de posibles víctimas en un ataque de esta naturaleza puede ser significativo, en ocasiones con miles de empresas afectadas.

Estos ataques son más difíciles de detectar si los proveedores no implementan un enfoque de seguridad proactivo, con políticas de seguridad adecuadas y herramientas de detección y respuesta que permitan identificar y actuar ante actividades sospechosas. Además, es importante que los proveedores cuenten con un procedimiento de respuesta ante incidentes para ataques a la cadena de suministro, y que este garantice la notificación a las entidades y a sus clientes, cuando proceda, con información precisa y oportuna.

Como conclusión, para determinar el nivel de exposición de una entidad resulta esencial identificar, supervisar y gestionar los riesgos derivados de las relaciones con sus proveedores externos de servicios tecnológicos.