COMILLAS
UNIVERSIDAD PONTIFICIA

Facultad de Ciencias Económicas y Empresariales

EL RIESGO DE OUTSOURCING: ANÁLISIS COMPARATIVO ENTRE REGULADORES

Autor: Marina Cañizares Marín
Director: Rafael Castellote Azorín

MADRID | abril 2021

Resumen

El ecosistema financiero ha experimentado una extraordinaria transformación en los últimos años, factores como la disrupción tecnológica o los intereses negativos, han hecho que la banca tradicional reinvente su modelo de negocio para sobrevivir. En este contexto, cobran importancia una serie de riesgos que, pese a no tener un origen estrictamente financiero, afectan de igual manera a las entidades del sector. Uno de estos riesgos deriva de las relaciones que las entidades financieras contraen con terceros ajenas a ellas y, más concretamente, de las relaciones de subcontratación o externalización de servicios. Las autoridades reguladoras y supervisoras de todo el mundo están atentas a la evolución de estos riesgos y con el objeto de proteger a sus entidades y, en especial, a sus consumidores, regulan estas relaciones de la mejor forma posible. Así, pese a sus diferencias, todas coinciden en la importancia de llevar una adecuada gestión de estos riesgos ya que el impacto que podría causar su falta de previsión supone una amenaza real para la estabilidad económica y financiera de los países.

Palabras clave: Riesgo no financiero, outsourcing, entidad financiera, regulador bancario, protección de datos, Unión Europea, Estados Unidos, Reino Unido.

Abstract

The financial ecosystem has undergone an extraordinary transformation in recent years, factors such as technological disruption or negative interests have made traditional banking reinvent its business model to survive. In this context, a series of risks become important which, despite not having a strictly financial origin, affect the sector's entities in the same way. One of these risks derives from the relationships that financial institutions enter into with third parties, more specifically, from the relationships of subcontracting or outsourcing services. Regulatory and supervisory authorities around the world are attentive to the evolution of these risks and, in order to protect their entities and, especially, their consumers, they regulate these relationships in the best possible way. Thus, despite their differences, they all agree on the importance of properly managing these risks since the impact that their lack of foresight could cause poses a real threat to the economic and financial stability of the countries.

Key words: Non-financial risk, outsourcing, financial institution, banking regulator, data protection, European Union, United States, United Kingdom

Índice

Índice de Tablas

Glosario de abreviaturas

EBA: European Banking Authority

OCC: Office of the Comptroller of the Currency

PRA: Prudential Regulation Authority

DORA: Digital Operation Resilience Act

EE. UU.: Estados Unidos

FSB: Financial Stability Board

TI: Tecnología de la Información

TIC: Tecnología de la Información y las Comunicaciones

BPO: Business Process Outsourcing

BCE: Banco Central Europeo

JST: Joint Supervisory Teams

UE: Unión Europea

MUS: Mecanismo Único de Supervisión

FPC: Financial Policy Committee

CEBS: Committee of European Banking Supervision

FAQ: Frequently Asked Questions

SS: Supervisory Statement

PS: Policy Statement

CAPÍTULO I - INTRODUCCIÓN

1. Planteamiento

Históricamente, el sector de la Banca ha prestado mucha atención a los riesgos de carácter financiero, como pueden ser los riesgos de liquidez, de mercado o de crédito; riesgos que, sin duda, afectan a la actividad financiera de forma sistémica y que incluso pueden llegar a suponer un grave perjuicio en los mercados si no se lleva a cabo un control efectivo de los mismos. Sin embargo, en una realidad donde los tipos de interés rozan dígitos negativos y la tecnología se apodera de las organizaciones tradicionales dando lugar a un nuevo modelo de negocio altamente digitalizado y automatizado, no se puede ignorar que surgen riesgos que hasta el momento no requerían la atención que actualmente demandan.

Nos referimos a los riesgos no financieros, aquellos que no tienen un origen estrictamente financiero pero que afectan de igual manera a las entidades que sí se dedican a la concepción y comercialización de productos financieros. Este tipo de riesgos como, el de Ciberseguridad, el operacional o el estratégico, han ido cobrando especial relevancia a lo largo de los últimos años. Las autoridades supervisoras y reguladoras del sector están especialmente alerta al respecto, y han materializado esta preocupación en directrices, reglamentos, normas de conducta y demás instrumentos normativos cuyo objetivo es el de ayudar a las entidades a la localización, evaluación y mitigación de estos riesgos antes de que puedan suponer efectos irreversibles para las mismas.

En este contexto, las autoridades han tomado la iniciativa para establecer marcos regulatorios que den respuesta a la nueva realidad del sector, proponer mecanismos de gestión y armonizar las prácticas empresariales con el objetivo de dar una respuesta consolidada que proteja a sus entidades y sobre todo a los usuarios de las mismas. Así, van surgiendo respuestas coordinadas a nivel global que pretenden contribuir a la resiliencia[1]operativa de los sectores financieros.

[1] capacidad de respuesta desde las operaciones ante situaciones operativas adversas y de recuperación ante disrupciones operacionales

2. Objetivos

El propósito del presente Trabajo de Fin de Grado es el de analizar los riesgos no financieros que afectan actualmente al sector financiero y, en concreto, los aspectos relativos al riesgo de externalización de servicios u *outsourcing* de las entidades financieras, es decir, los riesgos que se derivan de contratar servicios con terceros ajenos a la entidad. Para ello, se abordará la problemática desde un punto de vista normativo y se hará una exposición del tratamiento de este problema por parte de las autoridades supervisoras y regulatorias. En concreto se hará una comparación de lo que la Autoridad Bancaria Europea, la Autoridad Prudencial Regulatoria del Reino Unido y la Oficina del Controlador de la Moneda en EE. UU. contemplan en sus respectivas normativas acerca del riesgo de la externalización de actividades y servicios para las entidades financieras. Se llevará a cabo una exposición de las distintas normativas y un análisis en profundidad de su diferencias y puntos en común. Por último, se expondrá la visión de futuro y cómo en concreto la Unión Europea pretende abordar estas cuestiones a medio plazo con su nueva propuesta de reglamento DORA.

3. Metodología

La metodología empleada para la realización del presente el trabajo se basará en un análisis cualitativo de las bases de datos y fuentes bibliográficas existentes que traten este tema concreto de la forma lo más exhaustiva posible. Se llevará a cabo una recopilación y análisis crítico de la información disponible, que permitirá el análisis comparativo y descriptivo del estado del tema en cuestión. Para ello, acudiremos a fuentes normativas y demás documentos informativos que analicen la problemática de las entidades financieras en sus relaciones con terceros.

CAPÍTULO II - MARCO TEORICO

1. Sobre la actividad de Externalización (*Outsourcing*)

Para comprender de manera preliminar la problemática que queremos abordar en este trabajo debemos comenzar exponiendo el concepto de *outsourcing* y de qué maneras éste afecta hoy en día a las entidades financieras.

Podemos definir el *outsourcing* como la externalización de actividades ya sean de índole productiva como comercial, bajo un planteamiento de cooperación en las relaciones existentes entre las personas, o como la acción de recurrir a una agencia exterior para realizar una función que anteriormente se realizaba dentro de la empresa por lo que se transfiere tanto la planificación, administración y desarrollo de dicha actividad a una tercera parte independiente.[2] De este modo, las empresas pueden externalizar actividades con el fin de que otra empresa más especializada realice esta tarea de forma más eficiente, ahorrando así en costes, siendo esta actualmente la primera razón de externalización por parte de las empresas

En el sector financiero, al igual que en muchos otros, el *outsourcing* está a la orden del día, por ello, las autoridades bancarias comienzan a prestar especial atención a este tipo de actividades. El *Joint Forum* da una definición de *outsourcing* en sus directrices de febrero de 2005 en las cuales dedica un apartado a la externalización de servicios financieros. Según estas directrices, se define el outsourcing como "el uso de un tercero por parte de una entidad regulada (ya sea una entidad afiliada a un grupo corporativo o una entidad externa al grupo corporativo) para realizar actividades de manera continua que serían normalmente realizadas por esta entidad regulada, ahora o en futuro"[3]. Esta definición es tomada como punto de partida por muchas autoridades reguladoras en la elaboración de sus propias directrices, más adelante se llevará a cabo una comparación de estas definiciones y una exposición comparada de su relevancia.

Una de las razones por las que la Banca recurre a la externalización de sus operaciones es la creciente disrupción tecnológica, la cual ha revolucionado el ecosistema financiero tal y como lo conocíamos hace unos años. La aparición de empresas

[2] Romero, A. "Outsouring. Qué es y cómo se aplica" *Gestiópolis*, 19 abril 2002 (disponible en https://www.gestiopolis.com/outsourcing-que-es-y-como-se-aplica/ última consulta 14/04/2021)
[3] Discussion Paper FSB, 9th of November 2020, on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships

tecnológicas como las Fintech o Bigtech que proporcionan productos y servicios financieros más ágiles, baratos y accesibles, ha hecho que la banca tradicional se sumerja en un proceso de reestructuración y adaptación a un mercado cada vez más competitivo[4].

Otro gran factor que impulsa a las entidades financieras a decidirse por el *outsourcing* es la eficiencia en costes y la posibilidad de realizar actividades para las que el Banco (o la empresa en cuestión) no tiene el conocimiento o *expertise* suficiente. Así, los bancos encuentran en el *outsourcing* una vía por la que ahorrar en costes, tener acceso fácil a nuevas tecnologías y conseguir economías de escala.

Entre los distintos procesos o actividades que se pueden externalizar, lo habitual es que se lleve a cabo fundamentalmente con los servicios y tecnologías de la información (TI) y con la gestión de las relaciones con los clientes, siendo cada vez más común la externalización de procesos críticos y actividades de apoyo. Así, algunos ejemplos de *outsourcing* pueden ser los sistemas de gestión, la asistencia jurídica, actividades comerciales, tareas de procesamiento del cumplimiento o la formalización de operaciones de comercialización de productos, que se llevan a cabo mediante la contratación de proveedores externos como asesoras, gestoras, consultoras o empresas especializadas en *Business Process Outsourcing* (BPO).

2. Conceptos básicos

a. Riesgo no financiero

Entendemos por riesgos financieros todos aquellos que derivan de las transacciones que realiza una empresa y que implican la utilización de derechos de cobro y obligaciones de pago o aquellos que pueden surgir de las operaciones en los mercados financieros[5]. Tradicionalmente, son estos los riesgos que se tienen en cuenta al implementar estrategias de gestión empresarial, sin embargo, en los últimos años surgen

[4] ANDRÉS, R. "Un nuevo Ecosistema Financiero" *Cinco Días*, 29 de julio de 2015 (disponible en https://cincodias.elpais.com/cincodias/2015/07/29/economia/1438167270_377223.html última consulta 15/04/2021)

[5] EALDE, "Introducción a la Gestión de Riesgos Financieros" (disponible en https://www.ealde.es/gestion-de-riesgos-financieros/; última consulta 14/04/2021)

una serie de riesgos que, aunque no son nuevos necesariamente, suponen una amenaza muy patente para las instituciones financieras. Estos se conocen como riesgos no financieros y los podemos definir sensu contrario como aquellos que no tienen un origen financiero y, por tanto, no implican la utilización de derechos de cobro y obligaciones de pago, ni surgen de las operaciones en los mercados financieros[6].

Existen varios tipos de riesgos no financieros como el riesgo operacional, el reputacional, el estratégico, el tecnológico o, dentro de este último, el de ciberseguridad. Entre ellos, también encontramos el riesgo relacionado con la prestación de servicios en modalidad de *outsourcing* o pura prestación de servicios por terceros que será el objeto del presente estudio.

b. Riesgo Outsourcing

Como apuntábamos anteriormente, gracias a la externalización de servicios la banca tradicional consigue esa adaptación y reducción de costes que necesita para ser competitiva dentro del mercado actual, sin embargo, el outsourcing de este tipo de procesos en ningún caso supone la trasmisión de la responsabilidad ni del riesgo a los proveedores de estos servicios. Son las entidades las que responden de los fallos y déficits funcionales en los que puedan incurrir estos terceros ante los supervisores y reguladores bancarios que controlan este tipo de actividades y siempre pensando en la repercusión que esos errores pueden tener sobre los clientes finales.

La externalización de procesos y servicios en las entidades financieras está sometida a una carga regulatoria muy amplia. La presión sobre sus costes como palanca para incrementar la rentabilidad y la necesidad de centrarse en la diferenciación basada en la innovación[7] crean la necesidad de llevar este proceso de manera controlada y conforme a la propia estrategia de negocio. Una estrategia bien focalizada es capaz de brindarnos grandes oportunidades mientras que una estrategia desordenada puede hacer

[6] EALDE Business School, "Qué son los riesgos no financieros y cómo afectan a las empresas", *EALDE Business School* (disponible en https://www.ealde.es/riesgos-no-financieros/#:~:text=Qu%C3%A9%20es%20un%20riesgo%20no,inter%C3%A9s%2C%20sino%20de%20otro%20tipo; última consulta 14/04/2021)

[7] LASARTE.M "La externalización de la banca, bajo la lupa del BCE" *KPMG Tendencias* (disponible en https://www.tendencias.kpmg.es/2018/06/externalizacion-banca-bce/, última consulta 14/04/2021)

caer en riesgos de los que la propia entidad puede no ser consciente pudiendo llegar a perder completamente el control de su actividad frente a terceros[8].

Por tanto, es importante que las entidades identifiquen claramente los riesgos en los que pueden incurrir al externalizar actividades y tener controlados a sus proveedores, pues serán ellas las últimas responsables de los imprevistos que puedan suceder.

Así, cabe determinar el concepto de riesgo inherente y riego residual y la diferencia entre ambos. El inherente es aquel que las entidades tienen que mitigar, cuando el servicio lo presta un tercero, la mitigación se consigue vía certificación, lo cual supone el asegurar una serie de controles en todos los dominios de riesgo que correspondan sobre el proveedor. Aquel riesgo que queda sin mitigar es lo que conocemos como riesgo residual. De esta forma, el riesgo inherente es el que existe ante la ausencia de alguna acción que la Dirección pueda tomar para alterar tanto la probabilidad como el impacto del mismo[9], mientras que el riesgo residual es el riesgo que persiste después de esta acción o respuesta. El objetivo es que el banco o entidad financiera soporte unos riesgos residuales por debajo de lo que se denomina un "apetito de riesgo" razonable, pues el riesgo residual cero es en la práctica imposible ya que implicaría un coste infinito.

c. Reguladores y supervisores bancarios

En ocasiones, es posible que los mercados financieros fallen, lo cual puede llevar a que la población pierda la confianza en el sistema potenciando y alargando así la inestabilidad que se puede haber originado en un principio. Por ello, y con el fin de evitar que se produzca un colapso del sistema bancario, los Estados intervienen de dos formas distintas: estableciendo regulaciones y actuando a través de la supervisión.[10]

La regulación bancaria pretende asegurar el funcionamiento de las entidades financieras; se trata de crear una red que fortalezca a este tipo de entidades ante la posibilidad de que ocurran eventos desfavorables y armonizar así los intereses generales

[8] LASARTE.M "La externalización de la banca, bajo la lupa del BCE" *KPMG Tendencias* (disponible en https://www.tendencias.kpmg.es/2018/06/externalizacion-banca-bce/, última consulta 14/04/2021)
[9] Enterprise Risk Services "COSO Evaluación de Riesgos" *Deloitte*, noviembre de 2015.
[10] Banco de España "El papel de los Reguladores y Supervisores bancarios" *Aula Virtual Banco de España* (disponible en https://aulavirtual.bde.es/wav/es/menu/estabilidad-fina/reguladores/El_papel_de_los_2ba4c721ff0b651.html; última consulta 14/04/2021)

que puedan afectar directamente a las partes perjudicadas.[11] Se busca asegurar la solvencia y controlar los riesgos que puedan amenazar la estabilidad del sector. En este sentido, las autoridades prestan especial atención a las entidades sistémicas, es decir, aquellas tan grandes que si cayeran producirían un impacto muy grave e incluso podrían causar un colapso del sistema financiero[12]. Si este tipo de entidades quebrasen el efecto repercutiría en la economía real, un claro ejemplo de esto es la caída de *Lehman Brothers*, el banco estadounidense conocido por ser uno de los primeros síntomas de la crisis financiera en 2008.

Por su parte, la finalidad de la supervisión bancaria reside en velar por la estabilidad del sistema financiero asegurando la solvencia y el cumplimiento de la normativa dictada por los reguladores.

En cualquier caso, estas funciones se complementan entre sí para diseñar un sistema con información actualizada de la situación de las entidades financieras y su perfil de riesgos y poder adoptar medidas que mitiguen el impacto que pueden tener en la economía las crisis financieras que se puedan originar. Así, surgen organismos dedicados especialmente a mantener esta estabilidad. Para el objeto del presente estudio tendremos en cuenta: en Europa, el Banco Central Europeo y en concreto los Equipos Conjuntos de Supervisión (JST, siglas en inglés), en Estados Unidos la OCC (*Office of the Comptroller of the Currency*) y en Reino Unido la PRA (*Prudential Regulation Authority*).

i. Banco Central Europeo

Tras casi una década de negociaciones que ponen en marcha la Unión Económica y Monetaria en Europa, el 1 de junio de 1998 se crea satisfactoriamente el Banco Central Europeo compuesto por 11 países con las características necesarias para adoptar el euro como moneda única. El BCE surge con afán de una convergencia económica a través de la vigilancia multilateral de las políticas económicas de los Estados Miembros.[13]

---

[11] *supra*

[12] ÁLVAREZ, C. "¿Qué entidades forman parte de la lista de bancos sistémicos globales?" BBVA, 2020 (disponible en https://www.bbva.com/es/que-entidades-forman-parte-de-la-lista-de-bancos-sistemicos-globales/ última consulta 15/04/2021)

[13] Banco de España "Las tres fases de la UEM" *Banco de España* (disponible en https://www.bde.es/bde/es/secciones/eurosistema/uem/fases/Las_tres_fases_de_la_UEM-3b27baee75d0441.html; última consulta 14/04/2021)

A día de hoy, el Banco Central Europeo se encarga de dictar la política económica y monetaria en los 19 países de la Unión Europea que, actualmente, usan el euro. Se encarga de asegurar la estabilidad de precios manteniendo una inflación baja que ronde el 2% y garantiza la supervisión de las instituciones y mercados financieros por parte de las autoridades nacionales. Para cumplir con estos objetivos, el BCE lleva a cabo las siguientes funciones:

- Establece los tipos de interés a los que presta a los bancos comerciales de la zona euro
- Gestiona las reservas de divisas
- Promueve el funcionamiento adecuado de los sistemas de pago
- Autoriza la producción de billetes

En 2014, la supervisión prudencial de las entidades de crédito de los estados de la zona euro pasó a estar bajo el control del Mecanismo Único de Supervisión (MUS), liderado por el BCE. Sin embargo, el hecho más destacable derivado de esta nueva organización es la creación de los *Joint Supervisory Teams* (JST) pues son estos los encargados de la supervisión de las entidades financieras significativas.

El JST es responsable de hacer efectivas las actividades de supervisión a través de la ejecución del "proceso de revisión y evaluación supervisora del capital y la liquidez" (PRES), la preparación de un plan anual de evaluación supervisora y la ejecución de dicho plan[14]. Este organismo está formado por trabajadores del BCE y de las Autoridades Nacionales Competentes (ANC) de los países donde se encuentren las entidades en cuestión.

ii. *Office of the Comptroller of the Currency* (OCC)

En Estado Unidos es la OCC, en castellano la Oficina del Controlador de la Moneda, quien tiene la función reguladora y supervisora del sistema financiero, en

[14] TORRES, X. "El mecanismo único de supervisión y el papel de las autoridades nacionales" *Estabilidad Financiera Banco de España*, núm 29, 2015, p 29

concreto, autoriza, regula y supervisa todos los bancos nacionales y cooperativas de ahorro federales, así como las sucursales y agencias federales de bancos extranjeros, con la finalidad de asegurar que su funcionamiento sea seguro y cumpla con la ley. [15]

La OCC, al igual que el sistema bancario estadounidense, comienza a operar en el 1863 cuando el presidente Abraham Lincoln firma la Ley de Moneda Nacional (*National Currency Act*). Se crea así un sistema de bancos autorizados para emitir billetes a nivel nacional y se establece la OCC para administrar su funcionamiento, igualmente, se dota a este organismo con la capacidad de regular las actividades de préstamo e inversión de los bancos nacionales.

Actualmente, la OCC es una rama independiente del Departamento del Tesoro de los Estados Unidos que se financia mayoritariamente con las aportaciones que hacen los bancos nacionales y cooperativas de ahorro federales quienes pagan tarifas por el análisis y procesamiento de sus solicitudes corporativas.

Para cumplir con sus funciones supervisoras y reguladoras la OCC lleva a cabo las siguientes tareas[16]:

- Emitir regulaciones bancarias y proporcionar interpretaciones legales y orientación sobre las decisiones corporativas de las entidades
- Visitar y examinar las entidades que supervisa
- Evaluar las solicitudes para la creación de nuevas sucursales bancarias, para el cambio de estructura corporativa o de actividad de las entidades y evaluar las solicitudes de bancos extranjeros que desean operar dentro de los Estados Unidos
- Imponer medidas correctivas a las entidades que se encuentren bajo el gobierno de la OCC que no cumplan con las regulaciones o que de alguna forma se involucren en prácticas poco seguras.
- Proteger a los consumidores mediante la elaboración de leyes que aseguren un acceso justo y garanticen un trato igualitario

[15] "Oficina del Controlador de la Moneda" *USA gov* (disponible en https://www.usa.gov/espanol/agencias-federales/oficina-del-contralor-de-la-moneda; última vez consultado 14/04/2021)
[16] "About, OCC", *Office of the Comptroller of the Currency (OCC),* (disponible en https://www.occ.treas.gov/about/index-about.html; última consulta 14/04/2021)

iii. *Prudential Regulation Authority* (PRA)

El Banco de Inglaterra realiza las tareas de regulación y supervisión de las entidades financieras a través de la PRA, en castellano, Autoridad Reguladora Prudencial. Este órgano supervisa alrededor de 1.500 instituciones financieras con el fin de asegurar unos servicios y productos seguros para sus consumidores.

Después de la crisis financiera de 2008, el Gobierno de Inglaterra decidió hacer una reforma de su sistema financiero y es a partir de esta iniciativa como en 2013 acaba fundándose la PRA como regulador prudencial y autoridad supervisora en el territorio de Reino Unido. De este modo, y con el objetivo de promover y asegurar la seguridad de las instituciones financieras y de garantizar la competencia justa entre las entidades, la PRA lleva a cabo las siguientes funciones[17]:

- El procesamiento de las solicitudes de licencia que realicen las distintas entidades
- Supervisar las entidades financieras a través de un enfoque basado en el riesgo, lo cual implica supervisar las áreas que plantean mayores riesgos para el logro de los objetivos prudenciales.
- Imponer sanciones administrativas y multas financieras para garantizar el cumplimiento de las reglas
- Promover la seguridad de los fondos de los depositantes y asegurados y los intereses de los miembros y beneficiarios de las instituciones financieras. Una función esencial para asegurar la confianza en el sistema.

De esta forma la PRA junto con el FPC (*Financial Policy Committee*), ambas parte del Banco de Inglaterra, cooperan de manera coordinada para regular y garantizar la estabilidad financiera en Reino Unido. Mientras que la PRA se centra en la regulación micro prudencial, el FPC mantiene una visión más amplia centrándose en la regulación macro prudencial.

[17]"Functions of the Prudential Authority", *Prudential Regulation Authority*, (disponible en; https://www.bankofengland.co.uk/knowledgebank/what-is-the-prudential-regulation-authority-pra última consulta 14/04/2021)

CAPÍTULO III - Los reguladores bancarios frente al riesgo de outsourcing:

Como veníamos diciendo, la externalización de actividades en el sector financiero está a la orden del día, y serán los reguladores y supervisores bancarios los encargados de actualizar la normativa para garantizar que este tipo de prácticas se llevan a cabo de forma segura.

La regulación y supervisión de los riesgos no financieros relacionados con el *outsourcing* o externalización de servicios para las instituciones financieras es diferente según la jurisdicción en la que nos encontremos. Sin embargo, según el estudio realizado por el Consejo de Estabilidad Financiera (FSB, sus siglas en inglés) sobre la regulación y supervisión existente en este tema a nivel global[18], todas ellas comparten unos principios y objetivos similares y coinciden en la problemática que puede derivarse de los riesgos de *outsourcing*.

En primer lugar, los supervisores coinciden en que el hecho de externalizar una actividad o contratar a un tercero para realizar un servicio determinado no exime, en ningún caso, a la entidad financiera de la responsabilidad que pueda derivarse de esta actuación, de esta forma, será la entidad financiera la última responsable por cualquier actividad, función, producto o servicio que subcontrate o delegue en un tercero.

En segundo lugar, las autoridades están dedicando especial importancia dentro de este marco que es el *outsourcing* a los riesgos relacionados con la ciberseguridad, la protección de datos y el riesgo de continuidad operacional.

En tercer lugar, todas las autoridades han establecido una serie de requisitos o de expectativas que las entidades financieras tienen que cumplir a la hora de contratar servicios con terceros. En algunos casos incluso, la autoridad tiene cierto poder legal que le otorga potestad para acceder a datos, personal, instalaciones o sistemas de los terceros con el fin de recabar la información necesaria para poder ejercer sus funciones de regulación y supervisión.

Por otro lado, la FSB ha identificado también una serie de problemas o desafíos relacionados con la regulación y supervisión de las actividades de *outsourcing* y los riesgos derivados de las relaciones con terceros. Por ejemplo, las entidades financieras

[18] Discussion paper FSB, *op. cit*

deben asegurarse de que sus acuerdos contractuales con los proveedores les otorguen los derechos necesarios para acceder y obtener información de los terceros lo cual puede suponer dificultades en la negociación, sobre todo en los casos donde concurren distintas jurisdicciones.

Igualmente, existe una preocupación común entre las autoridades en torno a la posibilidad de que surja el riesgo sistémico derivado de la concentración en la prestación de algunos servicios por terceros. Este riesgo aumenta a medida que las entidades financieras delegan servicios críticos en un tercero determinado, así, el riesgo sistémico aumentaría si, por ejemplo, un número suficientemente grande de entidades financieras se volvieran dependientes de uno o un pequeño número de proveedores de servicios o de terceros subcontratados para la prestación de servicios críticos para la entidad que fueran difíciles de sustituir de forma eficaz en un plazo adecuado de tiempo. De ocurrir esto, un fallo o disfunción de alguno de estos proveedores podría derivar en consecuencias muy negativas para la estabilidad y seguridad financiera.

De este modo, teniendo en cuenta las dificultades mencionadas, entre otras, y dando especial importancia a la dependencia que este tipo de relaciones crea para las entidades con los terceros subcontratados, las autoridades reguladoras y supervisoras establecen una serie de medidas preventivas y correctivas en sus jurisdicciones correspondientes. En los siguientes apartados veremos, en concreto, el tratamiento por parte de las autoridades en los mercados principales: Europa, USA y UK.

1. Directrices EBA

En la Comunidad Europea, la actividad de *outsourcing* viene regulada por las directrices sobre externalización de la EBA (*European Bank Authority*) de 25 de febrero de 2019, que sustituyen las directrices que la CEBS *(Committee of European Banking Supervisors*) promulgó en 2006 únicamente para instituciones de crédito. Actualmente, las directrices EBA son de aplicación no solo a las instituciones de crédito e instituciones financieras sino también a las entidades de pago y de dinero electrónico. El objetivo es establecer unas directrices y recomendaciones dirigidas a las autoridades competentes y entidades financieras para poder constituir prácticas de supervisión coherentes, eficientes

y eficaces y garantizar una aplicación común, uniforme y coherente con el Derecho de la Unión[19].

Estas directrices, que son de aplicación desde el 30 de septiembre de 2019, prestan especial atención a los riesgos que derivan de contratar servicios tecnológicos con terceros, principalmente aquellos que tienen relación con la protección de datos y la ciberseguridad. Otro foco de atención va dirigido a la externalización de aquellas funciones que se consideran esenciales o importantes para la entidad, pues tendrán que cumplir con unos requisitos más estrictos ya que el *outsourcing* de este tipo de actividades tiene gran impacto en el perfil de riesgo de la institución en cuestión.

Las presentes directrices especifican los sistemas de gobierno interno, incluida la adecuada gestión de los riesgos, que las entidades, las entidades de pago y las entidades de dinero electrónico deberían aplicar cuando externalicen funciones, en particular en relación con la externalización de funciones esenciales o importantes. Se trata de que todos los riesgos asociados con el *outsourcing* sean identificados, evaluados, monitoreados, gestionados, reportados y, según corresponda, mitigados. En los siguientes apartados se llevará a cabo una breve descripción de los procedimientos y requerimientos establecidos para mitigar estos riesgos.

1. Concepto y evaluación

La Autoridad Bancaria Europea (EBA, sus siglas en inglés) define la externalización en su artículo 12 como el "*acuerdo de cualquier forma entre una entidad de pago o una entidad de dinero electrónico y un proveedor de servicios por el que dicho proveedor realiza un proceso, un servicio o una actividad que, de otro modo, serían realizados por la propia entidad, entidad de pago o entidad de dinero electrónico."* Del mismo modo, define al proveedor de servicios como la "*tercera parte que realiza un proceso, servicio o actividad que se ha externalizado, o partes de los mismos, con arreglo a un acuerdo de externalización*."

[19] Directrices EBA, 25 de febrero de 2019, sobre Externalización (EBA/GL/2019/02)

Para llevar a cabo una correcta aplicación de las directrices, las entidades y entidades de pago tendrán que determinar si el acuerdo que han realizado con un tercero se ajusta correctamente a esta definición de externalización, descartando aquellas funciones que por su naturaleza no se podrán considerar *outsourcing* en ningún caso, como puede ser una auditoría legal, las infraestructuras de red globales como Visa o MasterCard o los servicios de información de mercado suministrados por compañías como Bloomberg o Moody's.[20]

Dentro de esta evaluación, la entidad deberá considerar si la función que se externaliza se hace de forma recurrente o continua y si la función en cuestión se podría incluir entre las funciones que normalmente realizaría una entidad financiera. Así, la entidad deberá considerar en su evaluación todos los aspectos del acuerdo sin incluir, en ningún caso las siguientes funciones (Título II.3.28):

- Aquellas funciones que legalmente deben de realizarse por un proveedor de servicios;
- Los servicios de información de mercado;
- Las infraestructuras de red globales;
- Los acuerdos de compensación y liquidación entre cámaras de compensación, entidades de contrapartida central y entidades de liquidación y sus miembros;
- Las infraestructuras de mensajería financiera globales sujetas a la vigilancia de las autoridades pertinentes;
- Los servicios de corresponsalía bancaria; y
- La adquisición de servicios que no serían asumidos de otro modo por la entidad (limpieza, jardinería, servicios administrativos, etc.)

Por otro lado, la EBA establece el principio de proporcionalidad, de forma que las entidades y las autoridades competentes deberán tener este principio presente a la hora de desempeñar sus funciones. El principio de proporcionalidad tiene por objeto "*garantizar que los sistemas de gobierno, en particular los relacionados con la externalización, sean coherentes con el perfil de riesgo individual, la naturaleza y el modelo de negocio de la*

[20] Direcrices EBA, *op.cit.* artículo 28

entidad o la entidad de pago, y con la escala y complejidad de sus actividades, de manera que se alcancen eficazmente los objetivos de los requisitos regulatorios"[21].

De este modo, para cumplir con este principio de proporcionalidad, las entidades deberán tener presente la dificultad de las funciones externalizadas, los riesgos derivados del acuerdo, la esencialidad o importancia de la función externalizada y el posible impacto de la externalización sobre el resto de sus actividades. Igualmente, se habrá de tener en cuenta los criterios especificados en el título I de las Directrices EBA sobre el gobierno interno, así como lo establecido para ello en la Directiva 2013/36/UE.

2. Funciones esenciales o importantes

La EBA da especial importancia a la subcontratación o externalización de lo que se conoce como funciones esenciales o importantes, para ello, establece una serie de criterios a partir de los cuales las entidades deberán considerar si la función que están externalizando lo es. Así, se consideran que cumplen con las consideraciones de esencial o importante aquellas funciones que:

a) en el caso de producirse un fallo o anomalía de ejecución perjudicase de manera sustancial a: el cumplimiento continuado de las condiciones de su autorización u otras obligaciones y obligaciones regulatorias; a sus resultados financieros; a la solidez o continuidad de sus actividades bancarias y servicios de pago.

b) en el caso de externalizar tareas operativas relativas a las funciones de control interno, salvo que en la evaluación se determinase que un fallo en la ejecución de la función externalizada no traería repercusiones negativas en la eficacia de la función de control interno

c) en el caso de externalizar funciones de actividades bancarias o servicios de pago en la medida que se requeriría la autorización de una autoridad competente (por ejemplo, aquellas funciones relacionadas con la recepción de depósitos o de otros fondos financieros, la concesión de garantías, el arrendamiento financiero, y demás funciones enumeradas en el Anexo I de la Directiva 2013/36/UE)

[21] Directrices EBA, *op.cit.*, artículo 18

Por otro lado, para determinar si un contrato de outsourcing afecta a una función esencial o importante, las entidades también deberán considerar los resultados de la evaluación de riesgos considerando principalmente lo relativo al riesgo operacional. Igualmente, las entidades deberán prestar atención a factores como el impacto potencial de un fallo o interrupción en la función externalizada, la capacidad de control, cumplimiento o auditoría de la entidad sobre la función subcontratada[22] o la protección de datos y el impacto potencial de una vulneración de la confidencialidad.

La diferenciación entre las funciones esenciales o importantes y el resto de las funciones externalizadas es tan importante que tiene incluso que estar debidamente diferenciada en la política de externalización de las entidades.

En el acuerdo de externalización se habrá de detallar si se permite la subcontratación de funciones esenciales o importantes, de ser así el acuerdo escrito debería especificar: el tipo de actividad excluido de la subcontratación; las condiciones a cumplir; la obligación por parte del proveedor de garantizar el cumplimiento de sus servicios en todo momento; la autorización requerida para el tratamiento de datos; la obligación de informar en caso de cambio significativo en la subcontratación prevista; el derecho por parte de la entidad para oponerse a cualquier cambio significativo en la subcontratación de dichas funciones; y el derecho de la entidad para resolver el acuerdo en caso de subcontratación indebida.

3. Seguridad de los datos y sistemas

A la hora de subcontratar servicios con terceros, las entidades deberán asegurarse de que los terceros cumplen con los estándares de seguridad informática necesarios. Cuando sea oportuno, será preciso definir estos requisitos de seguridad dentro del acuerdo de externalización y llevar a cabo un seguimiento del cumplimiento de dichos requisitos. En el caso de tratarse de servicios en la nube u otros acuerdos que impliquen el tratamiento o la transferencia de datos personales, las entidades deberán adoptar un enfoque basado en el riesgo en relación con las localizaciones de almacenamiento y el procesamiento de

[22] "La EBA publica sus directrices revisadas para acuerdos de subcontratación" ,*finReg 360*, AR/2019/014 (disponible en https://finreg360.com/alerta/la-eba-publica-sus-directrices-revisadas-para-acuerdos-de-subcontratacion/; última consulta 14/04/2021)

los datos y con las cuestiones relativas a la seguridad de la información[23]. Por otro lado, las entidades deberán tener presente las diferentes regulaciones nacionales en materia de protección de datos pues habrán de asegurar que los acuerdos cumplan con todos los requisitos legales estipulados.

Las directrices EBA sobre la externalización de servicios no entran en demasiado detalle a la hora de regular la seguridad de datos y sistemas, enfatizan que se trata de una parte muy delicada y con la que se debe tener especial cuidado en los contratos de externalización, pero no se extiende demasiado en su regulación. Para ello tenemos las Directrices EBA sobre la gestión de riesgos TIC y de seguridad (EBA/GL/2019/04) que completan el marco regulatorio de la materia. De este modo, las directrices establecen en su artículo octavo que para garantizar la continuidad de los servicios y sistemas de TIC, las entidades financieras deberán asegurarse de que sus contratos con los proveedores incluyen los objetivos y medidas apropiados y proporcionados a los procesos de cifrado de datos, seguridad de red y seguimiento de la seguridad, así como a la ubicación de los centros de datos. Igualmente, deberán incluir los procedimientos de gestión de incidentes de seguridad y operativos incluyendo los canales de comunicación y el escalado. Así, las entidades serán responsables de controlar y garantizar el nivel de cumplimiento de los objetivos de seguridad, las medidas y los objetivos de rendimiento por parte de dichos proveedores (art.9).

2. Directrices OCC

La Oficina del controlador de la Moneda publica sus recomendaciones para guiar a los bancos nacionales en USA a la hora de detectar y manejar los riesgos asociados a los contratos con terceras partes en su boletín 2013-29, del 30 octubre de 2013. Se trata de una serie de pautas que la OCC recomienda para externalizar servicios o actividades de manera segura, pese a que su publicación es del 2013 el boletín permanece vigente, si bien la OCC ha publicado en reiteradas ocasiones boletines con cuestiones que se preguntan frecuentemente (FAQ) cuya finalidad es la de suplementar el boletín de 2013 y aclarar las dudas que puedan surgir dada la rápida evolución dentro de la industria. Por

[23] Directrices EBA, *op.cit*, artículo 83

ello, a lo largo del análisis nos apoyaremos también en el boletín 2020-10 publicado el 5 de marzo de 2020.

La autoridad bancaria estadounidense establece una serie de prácticas que las entidades bancarias deberán tener presentes a la hora de subcontratar servicios con terceros pues, como reitera el organismo a lo largo de todo el texto, el hecho de delegar actividades en terceras partes no exime en ningún caso de la responsabilidad que puede contraer la entidad bancaria del desempeño de sus funciones.

Igualmente, la OCC presta especial atención al *outsourcing* de actividades críticas, o como decíamos en el apartado anterior, las llamadas actividades esenciales o importantes. Así, la OCC espera que los bancos tengan procesos de gestión de riesgos adaptados al nivel de riesgo y la complejidad de cada actividad subcontratada y en consonancia con la estructura organizacional del banco.

1. Concepto y evaluación

La oficina del controlador de la Moneda define las 'relaciones con terceros' (*third-party relationship*) como cualquier acuerdo de negocio entre la entidad bancaria y otra entidad ajena[24]. Dicho esto, podría incluirse dentro de esta amplia definición cualquier actividad que implicase la externalización de actividades o servicios, el uso de consultores independientes, acuerdos de *networking*, servicios de procesamiento de pagos, servicios prestados por filiales y subsidiarias, empresas conjuntas o Joint Ventures, y demás acuerdos comerciales en los que la entidad bancaria mantiene una relación continuada en el tiempo o puede llegar a contraer responsabilidad de los riesgos asociados. En términos generales, únicamente se excluirían las relaciones con los clientes dentro de esta clasificación.

La verdadera preocupación de la OCC es que la calidad de la gestión del riesgo no esté a la altura del nivel de riesgo y la complejidad de las relaciones con terceros y, por ello, establece un 'ciclo de vida' para la gestión efectiva de estos riesgos que incluye las siguientes fases:

[24] OCC Bulletin 2013-29, october 30th 2013, Third-Party Relationships: Risk Management Guidance

- Planificación: El desarrollo de un plan para gestionar la relación con el tercero, llevar a cabo las diligencias debidas para garantizar que la entidad selecciona a un tercero adecuado y entiende y controla los riesgos que plantea la relación.
- Negociación del contrato: Elaborar un contrato que defina con claridad las expectativas y responsabilidades del tercero y realizar un seguimiento continuo de la relación con el tercero una vez firmado el contrato.
- Terminación: Desarrollar un plan de contingencia que garantice que el banco puede transferir las actividades a otro tercero, incorporar las actividades a la empresa, o interrumpir las actividades cuando un contrato expire, se hayan cumplido los términos del contrato, en respuesta al incumplimiento del contrato, o en respuesta a cambios en la estrategia de negocio del banco o del tercero.

Además, la entidad bancaria deberá realizar a lo largo de todo el ciclo tareas de supervisión y rendición de cuentas o responsabilidad, de documentación en información y de revisiones independientes del proceso de gestión de riesgos. Así, la OCC recomienda que la administración de la entidad determine los riesgos asociados con cada relación con terceros para, posteriormente, poder determinar cómo ajustar las prácticas de administración de riesgos para cada relación en concreto.

2. Funciones esenciales o importantes

La autoridad bancaria estadounidense da especial importancia a la gestión de riesgos de las llamadas actividades 'críticas' de forma que establece un procedimiento adaptado para valorar, controlar y gestionar estos riesgos, incluso recomienda que se considere la posibilidad de nombrar un cargo específico para supervisar el correcto desarrollo de la actividad crítica subcontratada. De este modo, establece como actividades 'críticas' aquellas que afectan a funciones bancarias significativas como por ejemplo pagos, liquidaciones o custodias, aquellas que afecten a servicios compartidos significativos, como puede ser la tecnología de la información y aquellas actividades que:

- Pudiesen causar un riesgo significativo si la tercera parte fallara en el desarrollo de la actividad o no cumpliese las expectativas.

- Pudiesen causar un impacto significativo en los clientes
- Requirieran grandes desembolsos de dinero en recursos para llevar a cabo el acuerdo y gestionar el riesgo
- Pudiesen tener un gran impacto en las operaciones de la entidad si ésta tuviese que encontrar una tercera parte alternativa o si la actividad externalizada tuviese que ser llevada a cabo internamente.

Como parte de la supervisión continua, la dirección de la entidad bancaria debe evaluar periódicamente las relaciones existentes con terceros para determinar si la naturaleza de la actividad realizada constituye una actividad crítica. Mientras que algunos bancos asignan un nivel de criticidad o riesgo a cada acuerdo que mantienen con terceros, otros identifican las actividades que consideran críticas y los terceros asociados a ellas. La OCC acepta como válidos cualquiera de los dos enfoques pues, como aclara en su boletín 2020-10, no toda relación que implique actividades críticas es necesariamente una relación crítica con un tercero. Por tanto, la mera participación en una actividad crítica no convierte necesariamente a un tercero en un tercero crítico. Es común que la entidad tenga varias relaciones con terceros que sirvan de apoyo para una misma actividad crítica pero no todas estas relaciones serán críticas para el éxito de esa actividad en particular. Así, la OCC establece que sea cual sea el enfoque de la entidad bancaria, éste debe contar con una metodología sólida para designar qué relaciones con terceros recibirán una supervisión y una gestión del riesgo más rigurosas y exhaustivas.

En suma, la OCC establece una serie de criterios para identificar las actividades 'críticas' pero serán el consejo de administración y la dirección de la entidad los encargados de decidir si la actividad subcontratada con el tercero en cuestión es crítica o no, es el consejo de administración el encargado de aprobar las políticas y los procedimientos que abordan cómo se identifican las actividades críticas.

Por otro lado, el boletín establece una serie de consideraciones que se deberán tener presentes a lo largo del proceso de gestión de riesgos cuando se trate de actividades críticas. Por ejemplo, cuando la relación con un tercero implique una actividad crítica será necesario llevar a cabo una diligencia debida más amplia cuyos resultados deberán ser presentados al consejo de administración pues será el consejo quien apruebe este tipo de relaciones antes de su ejecución. Esto significa que se debe facilitar al consejo la información necesaria para entender la estrategia que la entidad desea seguir al

externalizar actividades críticas para así poder identificar los beneficios y los riesgos asociados al contrato en cuestión y poder aprobarlo.

3. Seguridad de los datos y sistemas

En caso de que la relación con el tercero implicase el uso de sistemas tecnológicos y datos personales, la OCC recomienda a las entidades que antes de embarcarse en dicha relación contractual se obtenga una comprensión clara de los procesos comerciales y la tecnología de terceros que se utilizará para respaldar la actividad. Cuando la tecnología sea un componente importante de la relación establecida será recomendable que se revisen los sistemas de información de la entidad y del tercero para identificar brechas que puedan abrirse en las expectativas de nivel de servicio, tecnología, procesos comerciales y de gestión, o problemas de interoperabilidad. También será aconsejable revisar los procesos del tercero para mantener inventarios precisos de su tecnología y subcontratistas, así como, evaluar los procesos de gestión de cambios del tercero para asegurarse de que existen roles, responsabilidades y segregación de funciones y que se establecen de forma clara. Por último, se sugiere comprender las métricas de desempeño del tercero para sus sistemas de información y asegurarse de que cumplen con las expectativas de la entidad bancaria.

Por su parte, la OCC aclara en su boletín FAQ de 2020 que la gestión de riesgos de terceros para los servicios en la nube es fundamentalmente la misma que para otras relaciones con terceros. El nivel de diligencia debida y de supervisión deberá ser acorde con el riesgo asociado a la actividad o los datos que se manejan en la nube. Se deberá tener una clara comprensión de la división establecida entre los controles que el proveedor de servicios de la nube es responsable de gestionar y los controles que la entidad bancaria deberá configurar y administrar independientemente y como última responsable.

En cuanto a la gestión de datos personales, el boletín 2020 aclara que un banco que tiene un acuerdo comercial con un agregador de datos tiene una relación con un tercero y, por tanto, el nivel de diligencia debida y la supervisión continua deberán ser proporcionales al riego para el banco. La seguridad de la información debe ser un punto clave en la gestión de riesgo de terceros pues una brecha de seguridad en el sistema puede

causar daño a los clientes y puede causar un riesgo de reputación y seguridad y responsabilidad financiera a la entidad.

3. Directrices PRA

La Autoridad de Regulación Prudencial (PRA, sus siglas en inglés) emitió un boletín de consulta en diciembre de 2019 cuyo objetivo era el de lanzar una propuesta regulatoria en la cual se desarrollasen las Directrices de la Autoridad Bancaria Europea en relación con la externalización de actividades u *outsourcing*, modernizando así el marco normativo del Reino Unido que regía hasta el momento la subcontratación y la prestación de servicios por parte de terceros. El documento de consulta establecía una serie de propuestas y abría paso a que las partes afectadas respondiesen y comentasen críticamente el proyecto desde un punto de vista práctico. Por consiguiente, en marzo de 2021, la PRA publicó su respuesta a estos comentarios estableciendo una política consolidada por el documento PS7/21[25] y en la Declaración de Supervisión (SS) 2/21 sobre "Outsourcing y gestión del riesgo de terceros"[26]. Así, queda establecida la SS2/21 como principal fuente de referencia para las entidades financieras a la hora de interpretar y cumplir con los requisitos de la PRA sobre la externalización y gestión del riesgo de terceros, si bien las directrices de la EBA, seguirán siendo de aplicación a todas las operaciones europeas de empresas británicas al igual que a las actividades realizadas por empresas en el marco europeo que tengan también presencia en el Reino Unido.

Con este documento, la Autoridad pretende facilitar una mayor resiliencia junto con la adopción de la nube y otras tecnologías nuevas, complementar los requisitos y las expectativas sobre la resiliencia operativa existentes en el Reglamento de la PRA, en el SS1/21 y la declaración de política (*Statement of Policy*) en materia de resiliencia operativa y, finalmente, implementar las Directrices EBA sobre externalización y, cuando sea relevante, las Directrices EBA sobre la seguridad y gestión de riesgos TIC.

Se trata de un documento recién publicado por lo que se espera que las entidades lo puedan cumplir para el 31 de marzo del año 2022. De esta forma, las entidades afectadas, es decir, las entidades a las cuales se dirige el documento son los bancos de

[25] PRA Policy Statement, March 2021, Outsourcing and third party risk management (PS7/21)
[26] PRA Supervisory Statement, March 2021, Outsourcing and third party risk management (SS2/21)

Reino Unido, las sociedades de crédito y empresas de inversión designadas por el PRA, empresas y grupos de seguros y reaseguros y las sucursales británicas de bancos y aseguradoras extranjeras[27]. Por su parte, algunos de los preceptos estarán también dirigidos a las cooperativas de crédito y las denominadas "*non-directive firms*"[28].

A través de este documento, la autoridad inglesa espera que queden regulados los acuerdos de *outsourcing* de cualquier tipo, los acuerdos con terceras partes distintos de *outsourcing* en determinados casos que queden indicados y la implementación de servicios en la nube en ocasiones concretas, para poder llevarlos a cabo de una forma segura y resiliente. Y, en concreto, se examinarán las cuestiones relativas a la seguridad de datos, el acceso, auditoría y derecho de información, el *sub-outsourcing* y las estrategias de salida y de continuidad de negocio.

1. Concepto y evaluación

El concepto de outsourcing viene definido en el artículo 2 del Reglamento de la PRA como un acuerdo de cualquier tipo entre una empresa y un proveedor de servicios ya sea una entidad supervisada o no, mediante el cual, dicho proveedor de servicios realiza un proceso, un servicio o una actividad, ya sea directamente o mediante subcontratación que, de otro modo, sería realizado por la propia empresa. En consonancia con las Directrices EBA, a la hora de determinar si un acuerdo con terceros queda dentro de esta definición, las empresas deberán considerar si el tercero realizará la función o el servicio en cuestión de una forma recurrente o continua.

Los requerimientos relativos al outsourcing no aplicarán a las relaciones que las entidades puedan contraer con terceras partes que no puedan ser incluidas dentro de la definición, si bien se espera que las entidades apliquen una gobernanza y unos controles adecuados a todas las dependencias de terceros que puedan afectar a sus objetivos estatutarios. De este modo, se recoge una lista de ejemplos de acuerdos entre las entidades y terceros que como regla general no se deberá de considerar como *outsourcing* donde se incluyen las compras de hardware, software y otros productos TIC o, en el caso de tratarse

[27] PRA Supervisory Statement, *op.cit.*, art. 1.2
[28] "*non-directive firms*" son aquellas entidades cuyos ingresos brutos por primas son interiores a 5 millones de euros y cuyas provisiones técnicas brutas son inferiores a 25 millones de euros

de una aseguradora, el uso de agregadores como las plataformas de comparación de precios. Además, se remite a la EBA para completar esta lista con los ejemplos que en sus Directrices se desarrollan.

Adicionalmente, se tiene en cuenta que, en ocasiones, los acuerdos con terceras partes que caigan fuera de la definición de *outsourcing* pueden suponer un impacto relevante para los objetivos de la Autoridad inglesa, por lo que se espera que en cualquier caso las entidades evalúen la materialidad y los riesgos que se puedan derivar de estas relaciones, independientemente de si se incluyen o no dentro de la definición de externalización.

En línea con lo que establece la Autoridad Bancaria Europea en sus Directrices, se establece la proporcionalidad como principio básico que deben seguir las entidades para aplicar de forma correcta lo recogido en el documento. Así, las entidades deberán cumplir con las expectativas propuestas de manera adecuada a su tamaño, organización interna, a su perfil de riesgo y a su naturaleza, alcance y complejidad de sus actividades, y a la criticidad o importancia de la función externalizada[29].

En el documento el PRA especifica cómo debería ser la política de externalización de servicios, no existe una política standard que pueda ser válida para cualquier empresa pues, en línea con el principio de proporcionalidad, las entidades deberán desarrollar una política de outsourcing que sea adecuada a su complejidad, su estructura organizacional y su tamaño. Sin embargo, se establece un contenido mínimo que toda política de *outsourcing* debería contener[30]como por ejemplo las responsabilidades de los miembros del consejo, un registro de las actividades que se externalizan en cada momento, los procesos de identificación, evaluación, gestión y mitigación de los potenciales conflictos de intereses, un plan de continuidad del negocio, los procesos de *due diligence* requeridos con anterioridad al acuerdo para poder evaluar el riesgo y la materialidad, un sistema de supervisión, los procesos y estrategias de terminación del acuerdo, entre otros.

2. Funciones esenciales o importantes

El Reglamento de la PRA advierte que no debemos confundir la proporcionalidad con la materialidad de los acuerdos externalizados ya que la proporcionalidad se centra

[29]PRA Supervisory Statement, *op.cit*., art. 3
[30] PRA Supervisory Statement, *op.cit.*, Table 3

en las características de la entidad y la materialidad en el impacto potencial de un acuerdo de externalización en concreto. Así, define la externalización de actividades "materiales" como la externalización de servicios de tal importancia que la debilidad, o el fracaso, de los mismos arrojaría serias dudas sobre la continuidad satisfactoria de la empresa en cuanto al umbral de condiciones o el cumplimiento de las Normas Fundamentales[31]. De este modo, la 'materialidad' evalúa el impacto potencial de un determinado acuerdo de externalización sobre la seguridad y la solidez de una empresa, incluida su resiliencia operativa. Dentro de esta definición, la autoridad reguladora incluye el concepto de funciones esenciales o importantes que se desprendía de las directrices EBA, anteriormente explicadas.

El capítulo dedicado a la materialidad es tan minucioso y extenso que, las entidades deberán remitirse a éste para encontrar el concepto y los criterios necesarios con los que evaluar la materialidad de sus contratos.

Las entidades son las responsables de evaluar cuándo una función externalizada adquiere el carácter de material, y deberán hacerlo previamente a la realización del contrato. Para ello, el PRA establece una serie de medidas para asegurar que la evaluación se lleva a cabo de forma satisfactoria. Por un lado, introduce criterios comunes para mejorar la coherencia de las evaluaciones de materialidad por parte de las empresas, si se cumpliesen alguno de esos criterios daría lugar a que el acuerdo de externalización de esa actividad en concreto se considerase material de manera automática. Así, deberán serán calificados como materiales, en términos generales, aquellos acuerdos que puedan perjudicar de manera sustancial a:

- La estabilidad financiera de UK,
- La capacidad de la entidad para cumplir con el umbral de condiciones (*Threshold Conditions*), cumplir con las Reglas Fundamentales, con los requisitos de la legislación pertinente y el Reglamento de la PRA, y que puedan afectar a la seguridad y solvencia de la entidad.
- En caso de aseguradoras, la capacidad de ofrecer un grado de protección adecuado a quienes sean los asegurados y que pueda afectar al requisito de no socavar el

[31] La PRA tiene ocho Normas Fundamentales que se aplican a todas las firmas autorizadas, son normas de alto nivel que actúan colectivamente como expresión del objetivo general de la PRA de promover la seguridad y solidez de sus empresas

servicio continuo y satisfactorio a los asegurados (de acuerdo con los objetivos legales del PRA)

- Si el acuerdo afecta a una actividad enteramente regulada
- Si afecta al 'control interno' o 'funciones claves', a menos que la entidad esté convencida de que un defecto o fallo de funcionamiento no afectaría negativamente a la función en cuestión.

Se espera, además, que las firmas tengan en cuenta todos los criterios que se exponen en la tabla 5 del artículo 5.13 del SS cuando se evalúe la materialidad de una actividad externalizada o un acuerdo con terceros

De igual forma, la autoridad reguladora espera que las empresas notifiquen los acuerdos de *outsourcing* de actividades materiales con suficiente antelación antes de su celebración para permitirles realizar un examen de supervisión adecuado. También espera que, una vez llegado a un acuerdo se incluya en éste, como mínimo: una descripción clara de la función externalizada, las fechas de inicio, renovación y fin, la ley gobernante, las obligaciones financieras, el *sub-outsourcing*, la localización del servicio, todos los aspectos relevantes en protección de datos, la supervisión, los niveles acordados de servicio, las obligaciones de notificación, y demás condiciones contempladas en el artículo 6.4 del documento.

3. Seguridad de los datos y sistemas

Dentro del término 'datos' la autoridad establece que se debe interpretar de forma muy amplia para que se incluyan los datos confidenciales, sensibles y transaccionales, así como los datos de fuente abierta[32] recogidos, analizados y transferidos con el fin de prestar servicios financieros y los sistemas utilizados para procesar, transferir o almacenar datos. Las expectativas contenidas en este capítulo serán de aplicación a los acuerdos de externalización de funciones materiales y demás relaciones con terceros que impliquen la transferencia de datos.

[32] Por ejemplo, los de las redes sociales

Por otro lado, la PRA espera que cuando el contrato implique la transferencia de datos, la entidad defina, documente y entienda sus responsabilidades y las de su proveedor respectivamente y que tomen las medidas adecuadas para protegerla.[33] De la misma manera, se espera que en este tipo de acuerdos las firmas clasifiquen los datos en función de su confidencialidad y sensibilidad; identifiquen los riesgos potenciales relativos a los datos y su posible impacto (legal, reputacional, etc.); se pongan de acuerdo en un nivel apropiado de accesibilidad, confidencialidad e integridad de los datos y; cuando fuese apropiado, obtuviesen las garantías y la documentación necesaria de terceros sobre la procedencia de los datos para poder asegurarse de que han sido recogidos y procesados de acuerdo con los requisitos legales y reglamentarios aplicables.

En el caso de servicios en la nube el término utilizado para ayudar a las empresas y a los proveedores de servicios en la nube a entender sus respectivas obligaciones es "modelo de responsabilidad compartida" [34]en el cual se define el modelo que debe operar en caso de externalizar servicios en la nube. Así, la entidad sería responsable del contenido que hay en la nube mientras que el proveedor de servicios lo es de la provisión de la nube, las entidades serían las responsables de identificar y clasificar correctamente los datos de acuerdo con sus obligaciones legales y reglamentarias y de determinar en qué jurisdicciones pueden almacenarse ciertos datos al igual que serán responsables de la configuración y la supervisión de sus datos en la nube para reducir los incidentes de seguridad y complimiento. Por su parte, los proveedores de servicios en la nube asumen la responsabilidad de la infraestructura que ejecuta el servicio externalizado (los centros de datos, hardware, software, etc.). Finalmente, ambas partes compartirán otras responsabilidades dependiendo del modelo de servicio.

[33] PRA Supervisory Statement, *op.cit.*, art.7.2
[34]PRA Supervisory Statement, *op.cit*., Table 5

CAPÍTULO IV - Análisis comparativo

Una vez realizada la síntesis de las distintas directrices dictadas por las autoridades regulatorias bancarias de Europa, Estados Unidos y Reino Unido, respectivamente en materia de *outsourcing*, llevaremos a cabo un análisis comparativo para identificar las principales diferencias existentes entre ellas. Así, examinando los conceptos más relevantes, llegaremos a un mejor entendimiento de lo que este tipo de 'recomendaciones' suponen en la realidad para las entidades financieras.

1. Concepto y ámbito de aplicación

Como veíamos anteriormente, las tres autoridades establecen una definición de outsourcing en torno a la cual desarrollan su texto reglamentario y a partir de la cual se determina su aplicabilidad a los posibles contratos que se lleven a cabo en las entidades.

De esta forma, la EBA define la externalización de actividades y servicios como "*el acuerdo de cualquier forma entre una entidad de pago o una entidad de dinero electrónico y un proveedor de servicios por el que dicho proveedor realiza un proceso, un servicio o una actividad que, de otro modo, serían realizados por la propia entidad, entidad de pago o entidad de dinero electrónico*[35]."

Por su parte, la Autoridad Reguladora Prudencial de Reino Unido la definía en su SS2/21 como "un acuerdo de cualquier tipo entre una empresa y un proveedor de servicios ya sea una entidad supervisada o no, mediante el cual, dicho proveedor de servicios realiza un proceso, un servicio o una actividad, ya sea directamente o mediante subcontratación que, de otro modo, sería realizado por la propia empresa"

Vemos que se tratan de definiciones muy similares y esto tiene que ver, en gran parte, con uno de los objetivos que define el PRA al publicar su boletín de consulta, el de implementar las directrices establecidas por la Autoridad Bancaria Europea para armonizar la regulación existente en la materia. Quizás la única diferencia que podemos identificar entre las definiciones es el ámbito de aplicación de cada una de ellas, es decir, quién se ve afectado directamente por cada una de las directrices. De esta manera, las

[35] *supra*

directrices EBA van dirigidas a las entidades de crédito, las entidades de pago y las entidades de dinero electrónico, si bien se establece en su artículo séptimo que están también destinadas a las autoridades competentes, y que estas deberán hacer todo lo posible para atenerse a ellas. Mientras, la PRA destina su informe a 'cualquier tipo de empresa' donde incluye bancos, aseguradoras, sucursales de bancos y aseguradoras en terceros países y, en algunos casos, a las cooperativas de crédito y lo que conocen como "*non-directive firms*".

Por su parte, la Autoridad estadounidense define las relaciones con terceros como "cualquier acuerdo de negocio entre la entidad bancaria y otra entidad ajena"[36]. Dentro de esta definición la OCC especifica que se puede incluir cualquier tipo de actividad que pueda implicar la externalización de actividades o servicios y expone toda una lista de actividades que la entidad bancaria puede contratar con un tercero, aclarando, que se considerará la condición de *outsourcing* siempre que se trate de una relación continua o de la que pueda tener responsabilidad por los registros asociados. Vemos, por tanto, una definición mucho más amplia que, en términos generales, únicamente excluiría las relaciones con clientes. Así mismo, la OCC alude únicamente a entidades bancarias refiriéndose con ello a los bancos nacionales, las asociaciones federales de ahorro, las sucursales federales y agencias de organizaciones bancarias extranjeras.

Por tanto, mientras que la EBA y la PRA contienen definiciones exhaustivas acerca de lo que constituye un acuerdo de externalización de actividades o servicios, la OCC, se centra en las relaciones con terceros desde una perspectiva mucho más amplia. Además, en las Directrices EBA se hace un listado de las actividades que, como principio general, las entidades no podrán considerar como externalización, listado al que la Autoridad inglesa se remite en sus directrices y que incluso amplía recordando que se tratan de ejemplos no limitados. Por el contrario, la OCC se limita a considerar cualquier acuerdo o contrato que la entidad contraiga con un tercero de manera continua sin excluir ninguna actividad en términos absolutos.

En este sentido vemos dos perspectivas distintas, de un lado la inglesa en consonancia con la europea y de otro la estadounidense, ya que la primera se centra principalmente en la actividad propia de *outsourcing*, definiendo perfectamente las relaciones que constituyen o no su ejercicio y la segunda se centra en dar un marco

[36] OCC Bulletin 2013-29, *op.cit.*

regulatorio a las entidades bancarias en materia de contratación con terceros donde se contempla, más bien, cualquier tipo de relación que éstas puedan contraer con terceros en el ejercicio de sus funciones.

Adicionalmente, cabe destacar que tanto las directrices EBA como las de la PRA establecen el principio de proporcionalidad como necesario para garantizar el cumplimiento efectivo de su contenido. La proporcionalidad difiere de la materialidad o esencialidad en que se centra en las características de la firma y no el tercero, se trata de garantizar que las medidas que toma la entidad para cumplir con las directrices sean coherentes con características como el perfil de riesgo individual, la naturaleza, la escala o la complejidad de sus actividades. Aunque la OCC no hace mención expresa al principio de proporcionalidad, se desprende de su boletín que las entidades bancarias deberán adoptar prácticas de gestión de riesgos acordes con el nivel de riesgo y la complejidad de sus relaciones con terceros, teniendo en cuenta las estructuras organizacionales de la entidad, por lo que, aunque en menor medida, la proporcionalidad queta también patente.

2. Funciones esenciales o importantes

Seguramente sea en este apartado donde encontremos mayor semejanza entre las tres autoridades, ya que cada una de ellas determina la importancia de identificar las actividades esenciales que se externalizan y establecen mecanismos de gestión específicos para identificar y prevenir los riesgos de una forma más efectiva. Cada autoridad las denomina de una forma, si bien ya sean conocidas como esenciales, materiales o críticas, todas coinciden en que son actividades a las que se debe especial atención por su carácter singular y por el impacto negativo que podría genera una mala gestión de su riesgo.

En las directrices EBA se denominan funciones esenciales o importantes y son tenidas en cuenta desde el principio de su redacción, pues incluso en el objeto de las mismas ya se adelanta que se pondrá especial atención a la externalización de funciones esenciales o importantes. De esta forma, la Autoridad Bancaria Europea dedica el Título 4 de sus directrices a este tipo de funciones, donde detalla de manera exhaustiva las situaciones que deberán ser consideradas como esenciales o importantes. Se lleva a cabo un análisis de las situaciones que pueden llegar a considerarse como tal teniendo en

cuenta, no solo el riesgo que conllevaría un fallo de las mismas sino también el impacto de estas actividades sobre las demás ramas del negocio y sobre los niveles de servicio previstos en relación con el riesgo operacional, riesgo de conducta, riesgo TIC, e incluso los riesgos reputacionales. Asimismo, se determina la responsabilidad por parte de las entidades de evaluar si una actividad se considera esencial o importante y la obligación de notificación a las autoridades competentes de forma previa al contrato[37].

De igual modo, la OCC referencia a las actividades que llama "críticas" desde un primer momento y, es que, como subraya en sus puntos destacados, el banco deberá garantizar la gestión integral de los riesgos y la supervisión de las relaciones con terceros que impliquen actividades críticas. De esta forma, la autoridad espera más rigurosidad a la hora de gestionar este tipo de actividades que define como significantes. A diferencia de las directrices EBA, la OCC no reserva ningún apartado para la identificación y consideración de las actividades críticas, se limita a definirlas en términos generales dando algunos ejemplos, es más, nos aclara en su boletín 2020-10 que las entidades podrán determinar el nivel de criticidad mediante la evaluación de cada una de las relaciones con terceros o mediante la identificación de las actividades críticas por sí y su relación con el tercero en cuestión y, añade, que no toda relación que implique actividades críticas será necesariamente una relación crítica con un tercero. Por ello, la OCC se limita a dejar un espacio de actuación para que las entidades establezcan sus métodos de identificación de actividades críticas, sentando unos criterios que deberán tomar a modo orientativo. No obstante, determina que la metodología para identificar dichas actividades debe de ser sólida pues las actividades críticas deben ser tenidas en cuenta en cada fase del ciclo de gestión de riesgos, donde se establece, según la fase, un trato especial y diferenciado del resto de actividades.

La autoridad inglesa se refiere a estas actividades con el calificativo de "materiales", pues considera que calificarlas como críticas o importantes puede suponer confusión con otros términos ya existentes en su regulación financiera. Su evaluación queda establecida dentro del Título 5 dedicado a la fase de pre-*outsourcing*, ya que se espera que las entidades determinen la materialidad de la actividad previamente al acuerdo para poder llevar a cabo una gestión correcta de la misma tomando las diligencias pertinentes. Así, define las actividades materiales como aquellas que tienen tanta importancia que la debilidad o el fracaso de las mismas arrojaría serias dudas sobre la

[37] Directrices EBA, *op.cit*, Art 58

capacidad de la empresa de seguir cumpliendo con el umbral de satisfacción previsto o las Normas Fundamentales[38]. Además, determina que este concepto debe ser completado teniendo en cuenta lo establecido para las actividades esenciales o importantes recogidas en la legislación de la Unión Europea. En consonancia con las Directrices EBA y a diferencia de lo recogido en el boletín de la OCC, la PRA realiza un detallado análisis de los criterios que pueden significar la materialidad de un servicio o actividad e incluso dispone que este concepto de materialidad y sus criterios se apliquen de manera general a todos los acuerdos con terceros.

Vemos por tanto que la esencialidad, criticidad o materialidad de las actividades y servicios que se externalizan o se contratan con terceros es de suma importancia para cada una de las autoridades. Las grandes diferencias se encuentran, de nuevo, entre lo establecido por la EBA y la PRA y lo establecido por la OCC. En este caso, las dos primeras se dedican a detallar minuciosamente las situaciones en las que se considera que una función es esencial y dan unos criterios muy similares que deberán ser incluidos en la evaluación de cada actividad en cuestión, en el caso de la PRA lo dispuesto en relación con la materialidad es tan completo y preciso que incluso se extenderá de manera general a todos los acuerdos con terceros que impliquen actividades materiales. La OCC, que no quita importancia a las actividades esenciales, establece menos criterios para su identificación, si bien es cierto que, al igual que las demás autoridades, las tiene en cuenta a lo largo de todo el ciclo de gestión de riesgos estableciendo el trato que deben darles las entidades en cada fase para llevar una adecuada gestión de su riesgo.

3. Seguridad de los datos y sistemas

Actualmente, como veíamos en apartados anteriores, cada regulación de externalización de servicios o relaciones con terceros contempla de forma más o menos extensa, cuestiones relacionadas con la seguridad de los datos y sistemas.

La Autoridad Bancaria Europea, no dedica muchos esfuerzos a regular este tema en sus directrices sobre la externalización, ya que lo aborda enteramente con sus directrices sobre la gestión de riesgos TIC y de seguridad. De esta forma, se refiere brevemente a ellos en el apartado 13.2 donde establece que se cumplan los estándares de

[38] PRA Supervisory Statement, *op.cit.*, art. 5.2

seguridad informática oportunos y que se definan requisitos en los acuerdos y se lleve un seguimiento adecuado de los mismos, sin perjuicio de lo establecido en otros reglamentos de la UE o disposiciones nacionales al respecto. Sin embargo

La autoridad inglesa, sin embargo, hace una evaluación más minuciosa de la seguridad de datos y de cómo deberían tratarse en materia de *outsourcing* y en relaciones con terceros. Así, la autoridad espera que las entidades clasifiquen los datos según su sensibilidad y confidencialidad, identifiquen los riesgos potenciales y sus impactos, acuerden un nivel adecuado de disponibilidad, confidencialidad e integridad de los datos y, cuando proceda, obtengan las garantías y documentación necesarias para asegurarse de que han sido procesados de acuerdo con los requisitos legales[39]. Se determinan también una serie de requisitos y procedimientos en relación con la clasificación de datos, la localización de datos y la seguridad de datos que se desarrollan a lo largo de todo su título séptimo.

Por su parte, la OCC hace referencia a la seguridad de los datos en su boletín de preguntas 2020-10 donde aclara cuestiones relativas a los servicios en la nube y la seguridad de los datos. No se trata de un análisis detallado en materia de protección de datos como veíamos anteriormente con la PRA pues se trata principalmente de cuestiones dirigidas a esclarecer los tipos de relaciones que se pueden constituir entre las entidades bancarias y los proveedores de la nube o agregadores de datos. El boletín aclara, que la seguridad de la información de ser un punto clave en la gestión del riesgo con terceros y explica que las entidades bancarias que tienen un acuerdo comercial con un agregador de datos o con un proveedor de servicios en la nube tienen una relación con un tercero y, por consiguiente, deberán llevar a cabo un nivel de diligencia y supervisión continua proporcional al riesgo que suponga para el banco.

4. Rango normativo y obligatoriedad

Por último, es interesante evaluar el carácter obligatorio, o no obligatorio, de estos boletines, es decir, hasta qué punto las autoridades y entidades financieras quedan vinculadas a lo establecido en estos textos. Pues bien, tanto las directrices EBA como el informe de supervisión de la PRA y el boletín de la OCC tienen carácter de

[39] PRA Supervisory Statement, *op.cit.*, art. 7.3

recomendación, en principio son textos que carecen de carácter normativo por lo que en ningún caso suponen requisitos de obligado cumplimiento cuya inaplicación resulte en un régimen sancionador. Sin embargo, cierto es que ni las autoridades nacionales ni las entidades afectadas pueden tomarse estas recomendaciones a la ligera.

En primer lugar, el Reglamento (UE) nº 1093/2010 por el que se crea la Autoridad Bancaria Europea[40] establece la facultad para emitir directrices y recomendaciones con la finalidad de promover la seguridad y la solidez de los mercados y determina que las autoridades competentes y las entidades financieras deberán hacer todo lo posible para cumplirlas. De esta forma, en el caso en que la autoridad competente o entidad no desease cumplir dichas directrices o recomendaciones debería emitir un informe detallado con las razones por las que no considera su adhesión, la EBA podría hacer públicos dichos motivos. Además, la Autoridad Bancaria Europea tiene el deber de informar al Parlamento Europeo, al Consejo y a la Comisión de las autoridades competentes que han decidido no cumplir las directrices en cuestión y habrá de proponer de qué forma piensa garantizar que en un futuro estas autoridades las cumplan (art.16.4).

La Autoridad Prudencial Regulatoria del Reino Unido emite lo que se conoce como "*Supervisory Statement*", documento de supervisión en castellano. Este tipo de documentos tienen la función de establecer marcos flexibles para las empresas, incorporando expectativas nuevas y existentes cuyo objeto es el de facilitar el juicio de las empresas y los supervisores para determinar si se cumplen o no esas expectativas. Por tanto, no se tratan de requisitos absolutos, ya que éstos solo se contemplan en las normas[41]. De esta forma, la autoridad espera que las entidades consideren las provisiones contempladas en el documento a la hora de establecer sus políticas de externalización, si bien únicamente quedarán sujetas estrictamente a aquellas que se remitan a leyes y demás requerimientos regulatorios, como lo establecido en el Reglamento de la PRA. Para estos casos, la autoridad sí que cuenta con una serie de medidas de ejecución entre las que se incluyen imposiciones y sanciones de todo tipo.

Por su parte, la OCC tiene el poder de tomar medidas de ejecución cuando se violen las leyes, normas o reglamentos, órdenes finales o condiciones impuestas por escrito; prácticas inseguras o poco sólidas y por el incumplimiento de las obligaciones

[40] Reglamento del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea) (No 1093/2010)

[41] "Policy", *Bank of England*, (disponible en https://www.bankofengland.co.uk/prudential-regulation/policy; última consulta 14/04/2021)

fiduciarias[42]. Dado que el boletín 2013-29 tiene por objeto proporcionar la orientación necesaria para que las entidades bancarias evalúen y gestionen los riesgos asociados a las relaciones con terceros y se espera que esto se lleve a cabo de manera efectiva junto con las demás regulaciones aplicables, entendemos que la palabra orientación en este caso sí que implica un obligado cumplimiento que, en mayor o menor medida, las entidades bancarias habrán de tener en cuenta a la hora de establecer y manejar sus relaciones con terceros.

[42] "Enforcement Actions", *Office of the Comptroller of the Currency* (disponible en https://www.occ.treas.gov/topics/laws-and-regulations/enforcement-actions/index-enforcement-actions.html última consulta 114/04/2021)

CAPÍTULO V- EL FUTURO

1. *Digital Operational Resilience Act* (DORA)

Como sabemos, el futuro se dirige hacia un mundo completamente digitalizado donde las entidades financieras dependerán íntegramente de las innovaciones tecnológicas para poder ofrecer productos y servicios seguros y ser capaces de desarrollar un modelo de negocio competitivo y sostenible. Por ello, para garantizar la resiliencia operacional de las instituciones, es decir, la capacidad de seguir prestando servicios y desarrollando su actividad ante los distintos escenarios adversos que se puedan dar, es necesario asegurar el funcionamiento de sus sistemas tecnológicos[43].

La Unión Europea ha hecho un importante ejercicio regulador para lograr este objetivo de resiliencia operacional y tecnológica al publicar a finales de septiembre de 2020 la propuesta de reglamento *Digital Operational Resilience Act* (DORA)[44] cuyo principal objetivo es el de mitigar los riesgos relacionados con la digitalización y garantizar así la resiliencia del sector financiero europeo. La propuesta forma parte del paquete de 'Finanzas Digitales', un conjunto de medidas para apoyar e impulsar el potencial de las finanzas digitales en términos de innovación y competencia, mitigando y gestionando los posibles riesgos que se derivan a su misma vez. Se trata de una nueva estrategia que la UE adopta con el objetivo de garantizar la revolución digital en Europa y de construir una economía preparada para el futuro cuyo funcionamiento sea seguro para los ciudadanos.

Al igual que veíamos en las Directrices EBA sobre el outsourcing, las reglas propuestas en el reglamento DORA se basan en el principio de proporcionalidad. Por un lado, tratan únicamente de cubrir aquellos aspectos que los Estados Miembros no pueden conseguir por ellos mismos, cuando la carga administrativa y los costes sean proporcionales a los objetivos específicos y objetivos generales que deban alcanzarse. Por otro lado, las nuevas reglas abarcan todo tipo de entidades financieras adaptándose, al mismo tiempo, a los riesgos y necesidades característicos de cada una de ellas en relación a su tamaño y perfil empresarial.

[43] Banco de España, "Novedades en la normativa relativa a los riesgos asociados a la tecnología y a su supervisión", *Recuadro 2.4, Memoria de Supervisión 2020,* pg. 64

[44] Proposal for a Regulation of the European Parliament and of the Council, 24th September 2020, on digital operational resilience for the financial sector (COM/2020/595 final)

La propuesta contiene requerimientos acerca de la gestión de riesgos vinculados a la tecnología, la gestión y notificación de incidentes tecnológicos, la comprobación de la resiliencia de los sistemas mediante pruebas y la gestión de sus relaciones con terceras partes[45], todo esto, a la vez que se fomenta la cooperación entre autoridades y la trasmisión de información entre instituciones.

Además, la propuesta abarca una amplia lista de entidades financieras reguladas a nivel de la Unión, donde entran entidades de crédito, entidades de pago, entidades de dinero electrónico, empresas de inversión, proveedores de servicios criptoactivos, depósitos centrales de valores, depósitos comerciales, gestores de fondos de inversión alternativos y empresas gestoras, proveedores de servicios de comunicación de datos, empresas de seguros y reaseguros, auditores legales y empresas de auditoría, proveedores de servicios de crowdfunding y demás empresas relevantes del sector financiero que recoge el artículo 2 del reglamento.

Como vemos, la propuesta supone un antes y un después en la regulación de ciberseguridad en Europa, se trata de un marco regulatorio mucho más extenso de lo que teníamos hasta el momento que goza de eficacia directa y establece un marco único de obligaciones, principios y requerimientos entre los que cabe resaltar lo relativo a los acuerdos entre las entidades financieras y terceros suministradores:

En primer lugar, el reglamento establece que las entidades financieras deberán contar con un marco de gestión de riesgos de TIC sólido, completo y bien documentado que les permita hacer frente a los riesgos de las TIC de forma rápida, eficiente y exhaustiva y garantizar un alto nivel de resistencia operativa digital que se ajuste a sus necesidades empresariales, tamaño y complejidad. Para ello, la autoridad espera que dentro de este marco se contemplen estrategias, políticas, procedimientos y demás herramientas necesarias para garantizar la seguridad de los datos e infraestructuras TIC. Este marco de gestión de riesgos TIC deberá ser revisado y documentado al menos una vez al año mejorándolo siempre en la medida de lo posible. Así, se define como riesgo de TIC cualquier circunstancia razonablemente identificable en relación con el uso de la red y los sistemas de información que, de materializarse, podría comprometer la seguridad de la red y los sistemas de información de cualquier herramienta o proceso dependiente de la tecnología, del funcionamiento y de los procesos, o de la prestación de servicios,

[45] *supra.*

comprometiendo así la integridad de los datos, los programas informáticos o cualquier otro componente de los servicios e infraestructuras de las TIC, causando una violación de la confidencialidad, un daño a la infraestructura física de las TIC u otros efectos adversos[46]

En segundo lugar, se hace referencia al riesgo de TIC frente a terceros, y se recoge que deberá gestionarse como un componente integral dentro del marco de gestión establecido para los riesgos TIC siguiendo siempre una serie de principios generales:

- La entidad financiera que externalicen servicios TIC será en todo momento plenamente responsables del cumplimiento de todas las obligaciones derivadas del reglamento y demás legislación aplicable
- La gestión de riesgos deberá implementarse siempre a la luz del principio de proporcionalidad
- El marco de gestión de riesgo de las TIC se revisará periódicamente, en especial, lo relativo a los riesgos identificados con respecto a la externalización de funciones críticas o importantes
- Las entidades deberán llevar a cabo un registro de información en relación con todos los acuerdos contractuales sobre los servicios TIC prestados por terceros, reportando a las autoridades los nuevos contratos que vayan surgiendo
- Previamente al acuerdo, las entidades financieras deberán: evaluar si afecta a una función crítica o importante, evaluar si las condiciones de supervisión se cumplen, identificar y evaluar todos los riesgos relevantes, llevar a cabo las diligencias debidas para asegurar que el acuerdo es adecuado e identificar y evaluar los posibles conflictos de intereses que los acuerdos pudiesen causar.
- Las entidades únicamente podrán celebrar acuerdos contractuales con terceros que cumplan con las normas de seguridad de la información más estrictas, apropiadas y recientes
- Se determinará de antemano, en función del riesgo, la frecuencia de las auditorías e inspecciones y las áreas que deben auditarse y, en caso de tratarse de funciones críticas, deberá verificarse la compatibilidad de los auditores

[46] Proposal European Parliament and Council, *op.cit*, art. 3.4

- Se deberán terminar los contratos en caso de cumplimento, circunstancias que así lo requieras identificadas durante las tareas de supervisión, en caso de deficiencias evidentes por parte del proveedor de servicios y cuando la autoridad competente no sea capaz de supervisar el acuerdo contractual.
- Se deberán establecer estrategias de salida exhaustivos y documentados en caso de surgir deficiencia o deterioro de la calidad de prestación del servicio

Por su parte, se establece un marco de supervisión para controlar continuamente las actividades realizadas por los llamados proveedores críticos, estos se determinarán en función de la dependencia que exista por parte del sector financiero hacia ellos junto con una serie de criterios cuantitativos y cualitativos que se designarán por la autoridad supervisora. La autoridad supervisora disfrutará de los poderes necesarios para llevar a cabo investigaciones y tener acceso a la información necesaria para poder llevar a cabo sus funciones.

En suma, la nueva regulación DORA supone nuevos principios y obligaciones que se suman al amplio marco que regula la actividad de las entidades financieras, se determinan obligaciones con repercusiones legales y sanciones y se lleva la seguridad de las redes y sistemas a un nivel avanzado para garantizar la seguridad de sus usuarios. Sin duda, la nueva normativa supondrá grandes cambios en los procesos internos de las entidades, que deberán adaptarse para obligatoriamente crear una cultura sólida de ciberseguridad interna.

CAPÍTULO VI - Análisis comparativo y conclusiones

En la siguiente tabla expondremos de manera visual las principales diferencias que existen entre las regulaciones objeto de nuestro estudio, incorporando en la comparación la nueva propuesta de reglamento DORA que, hasta el momento, no habíamos tenido en cuenta. El objetivo es valorar la importancia que las autoridades supervisoras y reguladoras dan a cada uno de los conceptos que hemos desarrollado en la comparación. Con importancia, nos referimos al nivel de regulación que ofrecen para cada caso guiándonos por criterios como la rigidez normativa, la exhaustividad de los conceptos expuestos o el nivel de cambio interno que las entidades habrían de afrontar para cumplir con las expectativas recogidas por las autoridades en cada caso concreto. Así, plasmaremos en la tabla, a través de colores, el esfuerzo que estas regulaciones esperan de las entidades afectadas, en otras palabras, nos servirá para entender el reto que afrontan las entidades financieras para cumplir con las previsiones establecidas en cada una de las regulaciones. Con este objetivo se asignarán los siguientes colores:

- Rojo: De suma importancia para la autoridad, supone un gran reto para la entidad dada la exhaustividad regulatoria. Las entidades deben tener en cuenta muchos requisitos para cumplir de manera satisfactoria las recomendaciones.
- Naranja: Muy importante y regulado por la autoridad, pero carece de procedimientos exhaustivos. Las entidades tienen mayor capacidad de decisión
- Verde: La autoridad establece un marco amplio y principios generales que deberán ser tenidos en cuenta

Tabla 1. Comparación ilustrativa

	Directrices EBA	Boletines OCC	SS2/21 PRA	DORA
Concepto outsourcing				
Funciones esenciales				
Datos y sistemas				
Obligatoriedad				

Fuente: elaboración propia

Llegamos a la conclusión de que quizá las directrices más laxas en materia de externalización son las que nos ofrece la autoridad estadounidense. Veíamos en los capítulos anteriores que, realmente, el boletín 2013-29 se centraba en la regulación de las relaciones entre entidades bancarias y terceros, deteniéndose brevemente en el concepto de *outsourcing*. Además, debemos tener en cuenta que se trata de un boletín publicado en 2013, por lo que en lo relativo a protección de datos y sistemas no hace demasiado hincapié ya que donde encontramos las respuestas a este tema es en los boletines de preguntas y respuestas que emite periódicamente, donde sí aclara algunas cuestiones con relación a la protección de datos sin entrar en demasiado detalle tampoco. En cuanto a la esencialidad o, en el caso de la OCC, criticidad de las funciones contratadas con terceros sí se establecen criterios más concretos y, es que, el boletín reitera en varias ocasiones la importancia que tiene una correcta evaluación de estas actividades, a las que les da un trato específico a lo largo de cada fase del ciclo de gestión que propone. Finalmente, en cuanto a la obligatoriedad, veíamos que pese a tratarse de unas recomendaciones y sugerencias la OCC tiene el poder de tomar medidas de ejecución cuando se violen las leyes, normas o reglamentos, órdenes finales o condiciones impuestas por escrito; prácticas inseguras o poco sólidas y por el incumplimiento de las obligaciones fiduciarias, por lo que, de algún modo, este boletín desprende cierta obligatoriedad para las entidades bancarias.

En cuanto a las Directrices EBA, veíamos que contienen preceptos muy completos y detallados acerca de lo que constituye el *outsourcing* y establecía requisitos y procesos que las entidades debían tener en cuenta a la hora de externalizar sus servicios. Estos requisitos y procesos son, incluso, más extensos cuando se trataba de funciones esenciales e importantes a las que se dedicaba un apartado entero dentro de sus directrices. Sin embargo, en lo relativo a datos y sistemas simplemente daba unas pinceladas de lo que se esperaba que las empresas considerasen en los acuerdos de externalización que afectaban a la protección de datos ya que, realmente, este tema es tratado en profundidad por otras regulaciones europeas como por ejemplo las Directrices EBA sobre la gestión de riesgos TIC y de seguridad. En cuanto a la obligatoriedad de su cumplimiento veíamos que únicamente tenían carácter de directrices, es decir, de guía o recomendación pues en ningún caso la autoridad competente o las entidades implicadas se ven vinculadas a lo recogido en el texto.

Por su parte, el *Supervisory Statement* de la PRA, supone un gran esfuerzo regulatorio ya que la autoridad inglesa trabaja duramente para publicar un documento que regule el *outsourcing* y las relaciones con terceros, recogiendo a su vez las recomendaciones europeas y estándares internacionales existentes en la materia. La PRA, recoge exhaustivamente los criterios de *outsourcing* y establece los procesos que las entidades deberán seguir para llevarlo a cabo, incluso debiendo notificar a la autoridad previamente a su compromiso. Podemos afirmar, que se le da mayor importancia a detección, evaluación y gestión de las actividades materiales incluso, ya que en el documento se sientan las bases para identificar el calificativo de material de todas las demás regulaciones, dicho de otro modo, el PRA espera que las entidades se remitan a estas recomendaciones cuando tengan que evaluar la materialidad de sus acuerdos, pese a no tratarse de acuerdos de *outsourcing*. Del mismo modo, se hace una minuciosa recopilación de los criterios que se deberán tener en cuenta a la hora de proteger los datos y trabajar con servicios en la nube. El SS tiene únicamente capacidad para establecer marcos flexibles para las empresas por lo que en ningún caso se trata de requisitos absolutos que éstas deban llevar a cabo, si bien debemos tener cuidado pues muchos de los preceptos establecidos en el documento se remiten a la ley y reglamentos, y estos, sí que tienen condición obligatoria.

Finalmente vemos que, si bien la regulación europea hasta ahora contemplada para la externalización de actividades y servicios no tiene rango normativo, la Unión ya ha

hecho pública la propuesta de regulación DORA *(Digital Operational Resilience Act)* que incluye preceptos en materia de externalización y más concretamente en externalización de servicios TIC. Esta propuesta se configura como un reglamento e incluso establece multas para su incumplimiento, por lo que sin duda la hace más estricta y obligatoria que las demás. Sin embargo, es cierto que se centra más en la ciberseguridad y los sistemas informáticos por lo que, aunque sí contempla preceptos en materia de *outsourcing*, su principal preocupación son los riesgos tecnológicos y de ciberseguridad.

1. Consideraciones Finales

Parte de las funciones de las autoridades reguladoras y supervisoras bancarias reside en su capacidad para anticipar escenarios que puedan afectar al sector financiero. De esta forma, las autoridades deberán estar alerta para asegurar que los riesgos que se puedan derivar de estos escenarios cuenten con una regulación y una supervisión adecuadas.

El crecimiento de empresas tecnológicas como las "Big Tech" en el sector financiero puede suponer una grave modificación de la estructura actual de nuestro sistema financiero, lo cual hace necesaria la previsión de riesgos y la regulación de los mismos para su mitigación. Otro ejemplo de la disrupción tecnológica deriva del desarrollo de los llamados criptoactivos, un medio digital de intercambio que se puede convertir en un sustitutivo del dinero "tradicional". La Autoridad Bancaria Europea ya ha tomado cartas en el asunto, publicando una propuesta de reglamento relativa a los mercados de criptoactivos[47]. Por otra parte, cada vez cobra más importancia el ámbito de las finanzas sostenibles y en este sentido también se pronuncia la Unión Europea al publicar el BCE en 2020 su Guía sobre riesgos relacionados con el clima y medioambientales[48].

El panorama financiero está sometido a un constante cambio y las autoridades regulatorias no pueden más que intentar adelantarse a ellos, sin embargo, esto no siempre es posible. Un claro ejemplo de ello es la situación de emergencia sanitaria que estamos

[47] Propuesta de Reglamento del Parlamento Europeo y del Consejo, 24 de septiembre de 2020, relativo a los mercados de criptoactivos (COM/2020/593 final)
[48] Banco Central Europeo, noviembre de 2020, Guía sobre riesgos relacionados con el clima y medioambientales

sufriendo a nivel global debido al COVID-19, un escenario de pandemia mundial que está afectando gravemente al sistema financiero y económico global. En este contexto, las autoridades deben proponer respuestas globales coordinadas para intentar mitigar los riesgos financieros, como son el de liquidez, el de mercado o el de crédito.

En este sentido la Autoridad Bancaria Europea ha llevado a cabo medidas como, por ejemplo, la publicación de las directrices de las moratorias (EBA (2020c)) o la relajación de los requerimientos sobre valoración prudente para evitar la excesiva volatilidad de los mercados financieros o la emisión de un comunicado por el que animaba a supervisores y reguladores a hacer uso de la flexibilidad existente en el marco regulatorio europeo para liberar capital[49].

2. Conclusión

Cualquier sector financiero robusto y consolidado –algo fundamental para la economía de cualquier Estado implica un papel preponderante por parte de las autoridades que lo regulan y supervisan.

Una de las funciones más relevantes de estas autoridades es la de prevenir todos los riesgos que puedan afectar a la continuidad operativa de las entidades que forman parte de este sector. Como hemos explicado a lo largo del trabajo, estos riesgos pueden ser de carácter financiero o no financiero, en función de su origen, siendo actualmente los riesgos no financieros los que surgen con más fuerza y aquellos sobre los que las autoridades empiezan a prestar más atención. En este contexto hemos analizado en particular el riesgo que se deriva de mantener acuerdos con terceros ajenos a las entidades o riesgo de *outsourcing*. Las autoridades de la Unión Europea, de los Estados Unidos y del Reino Unido han emitido respectivamente regulaciones con la finalidad de localizar, gestionar y mitigar estos riesgos que surgen de contratar con proveedores de servicios.

A lo largo del análisis, hemos comprobado que, en mayor o menor medida, todas ellas dan una respuesta estructurada centrándose principalmente en la externalización de las llamadas funciones esenciales, materiales o críticas y en la protección de datos y sistemas. Así, establecen medidas y ciclos de gestión para que las entidades afectadas

[49] ANGUREN, R., GUTIÉRREZ DE ROZAS, L., PALOMEQUE, E. y RODRÍGUEZ GARCÍA, C., "La respuesta regulatoria y supervisora frente a la crisis derivada del Covid-19" *Banco de España 2020,* pag 21

puedan llevar un control adecuado de este tipo de contratos evitando que pueda resultar en un quebranto para sus consumidores o para el sistema financiero en general.

En suma, tras haber analizado la respuesta que dan estas autoridades al riesgo de *outsourcing*, haber identificado sus principales diferencias y determinado el efecto que tienen sobre las entidades del sector, las conclusiones que podemos extraer son:

En primer lugar, las autoridades coinciden en que en la externalización de actividades y servicios las últimas responsables serán siempre las entidades financieras que lo contratan, por lo que en caso de que exista un fallo de cualquier tipo serán ellas las que se responsabilizarán en primera instancia y no el proveedor.

En segundo lugar, se le da mayor relevancia a la externalización de las denominadas funciones esenciales, críticas o materiales de las que se deberá llevar un mayor control y documentación en todo momento. Al igual que a los riesgos relacionados con la ciberseguridad y la protección de datos, para los que se prevén mecanismos especiales y adaptados en cada caso.

En tercer lugar, hablamos de directrices y recomendaciones que, pese a no tener un carácter estrictamente normativo u obligatorio, proponen unas prácticas que deberán ser tenidas en cuenta por las entidades en el desempeño normal de sus funciones.

Por último, la regulación de las relaciones que las entidades financieras contratan con terceros ajenos a ellas está a la orden del día, las autoridades dan una respuesta continua que no deja de actualizarse, un ejemplo de esto es la propuesta de reglamento DORA que hemos analizado. En este sentido, es responsabilidad de las entidades mantenerse permanentemente actualizadas y estar atentas a cualquier cambio legislativo para adaptar sus operativas y estándares de gobierno y control, con el fin de asegurar entornos operativos resilientes y razonablemente seguros para los clientes finales

CAPÍTULO VII - Bibliografía:

"About, OCC", *Office of the Comptroller of the Currency (OCC)*, (disponible en https://www.occ.treas.gov/about/index-about.html; última consulta 14/04/2021)

ÁLVAREZ, C. "¿Qué entidades forman parte de la lista de bancos sistémicos globales?" BBVA, 2020 (disponible en https://www.bbva.com/es/que-entidades-forman-parte-de-la-lista-de-bancos-sistemicos-globales/ última consulta 15/04/2021)

ANDRÉS, R. "Un nuevo Ecosistema Financiero" Cinco Días, 29 de julio de 2015 (disponible en https://cincodias.elpais.com/cincodias/2015/07/29/economia/1438167270_377223.html última consulta 15/04/2021)

ANGUREN, R., GUTIÉRREZ DE ROZAS, L., PALOMEQUE, E. y RODRÍGUEZ GARCÍA, C., "La respuesta regulatoria y supervisora frente a la crisis derivada del Covid-19" *Banco de España 2020*, pag 21

Banco Central Europeo, noviembre de 2020, Guía sobre riesgos relacionados con el clima y medioambientales

Banco de España "El papel de los Reguladores y Supervisores bancarios" *Aula Virtual Banco de España (*disponible en https://aulavirtual.bde.es/wav/es/menu/estabilidad-fina/reguladores/El_papel_de_los_2ba4c721ff0b651.html; última consulta 14/04/2021)

Banco de España "Las tres fases de la UEM" *Banco de España* (disponible en https://www.bde.es/bde/es/secciones/eurosistema/uem/fases/Las_tres_fases_de_la_UEM-3b27baee75d0441.html; última consulta 14/04/2021)

Banco de España, "Novedades en la normativa relativa a los riesgos asociados a la tecnología y a su supervisión", *Recuadro 2.4, Memoria de Supervisión 2020*, pg. 64

Directrices EBA, 25 de febrero de 2019, sobre Externalización (EBA/GL/2019/02)

Discussion Paper FSB, 9th of November 2020, on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships

EALDE Business School, "Qué son los riesgos no financieros y cómo afectan a las empresas", *EALDE Business School* (disponible en https://www.ealde.es/riesgos-no-

financieros/#:~:text=Qu%C3%A9%20es%20un%20riesgo%20no,inter%C3%A9s%2C%20sino%20de%20otro%20tipo; última consulta 14/04/2021)

EALDE, "Introducción a la Gestión de Riesgos Financieros" (disponible en https://www.ealde.es/gestion-de-riesgos-financieros/; última consulta 14/04/2021)

"Enforcement Actions", *Office of the Comptroller of the Currency* (disponible en https://www.occ.treas.gov/topics/laws-and-regulations/enforcement-actions/index-enforcement-actions.html última consulta 14/04/2021)

Enterprise Risk Services "COSO Evaluación de Riesgos" *Deloitte*, noviembre de 2015.

"Functions of the Prudential Authority", *Prudential Regulation Authority*, (disponible en; https://www.bankofengland.co.uk/knowledgebank/what-is-the-prudential-regulation-authority-pra última consulta 14/04/2021)

"La EBA publica sus directrices revisadas para acuerdos de subcontratación", *finReg 360*, AR/2019/014 (disponible en https://finreg360.com/alerta/la-eba-publica-sus-directrices-revisadas-para-acuerdos-de-subcontratacion/; última consulta 14/04/2021)

LASARTE.M "La externalización de la banca, bajo la lupa del BCE" *KPMG Tendencias* (disponible en https://www.tendencias.kpmg.es/2018/06/externalizacion-banca-bce/, última consulta 14/04/2021)

OCC Bulletin 2013-29, October 30th 2013, Third-Party Relationships: Risk Management Guidance

"Oficina del Controlador de la Moneda" *USA gov* (disponible en https://www.usa.gov/espanol/agencias-federales/oficina-del-contralor-de-la-moneda; última vez consultado 14/04/2021)

"Policy", *Bank of England*, (disponible en https://www.bankofengland.co.uk/prudential-regulation/policy; última consulta 14/04/2021)

PRA Policy Statement, March 2021, Outsourcing and third party risk management (PS7/21)

PRA Supervisory Statement, March 2021, Outsourcing and third party risk management (SS2/21)

Proposal for a Regulation of the European Parliament and of the Council, 24th September 2020, on digital operational resilience for the financial sector (COM/2020/595 final)

Propuesta de Reglamento del Parlamento Europeo y del Consejo, 24 de septiembre de 2020, relativo a los mercados de criptoactivos (COM/2020/593 final)

RAMÍREZ, M. R. G., GASCÓ, J. L. G., & TAVERNER, J. L. "Razones y riesgos del outsourcing de sistemas de información en las grandes empresas españolas". *Revista Europea de Dirección y Economía de la Empresa*, *24*(3), 2015, 175-189. ¿??

Reglamento del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea) (No 1093/2010)

ROMERO, A. "Outsouring. Qué es y cómo se aplica" *Gestiópolis*, 19 abril 2002 (disponible en https://www.gestiopolis.com/outsourcing-que-es-y-como-se-aplica/ última consulta 14/04/2021)

TORRES, X. "El mecanismo único de supervisión y el papel de las autoridades nacionales" *Estabilidad Financiera Banco de España*, núm 29, 2015, p 29