FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

LOS RIESGOS NO FINANCIEROS DE TERCEROS EN ENTIDADES FINANCIERAS Y LA COMPARACIÓN DE LA REGULACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES EN DISTINTAS REGIONES DEL MUNDO.

Autor: Natalia Villa Coduras
Director: Rafael Castellote Azorín

MADRID | junio 2023

RESUMEN

En el sector financiero, existe la posibilidad de que las entidades financieras puedan externalizar alguna de sus funciones o actividades y que éstas pasen a ser realizadas por un proveedor de servicios. Este proceso es comúnmente conocido como *outsourcing*.

Cuando las entidades financieras deciden externalizar una actividad es posible que se vayan a enfrentar a diferentes riesgos potenciales. En este caso se analizan los denominados riesgos no financieros los cuales no están relacionados con la gestión financiera, pero que pueden afectar de igual forma al funcionamiento de la entidad financiera.

El análisis se ha centrado en la comparativa de la regulación de los datos personales en el proceso de externalización en tres zonas distintas que son Europa, Estados Unidos y Reino Unido. Las autoridades reguladoras y supervisoras de cada zona analizada emiten unas directrices para todas las entidades financieras de esa zona sobre cómo debe de llevarse a cabo el proceso de externalización, y en especial, cómo se debe regular y proteger los datos personales de los clientes de la entidad financiera en el caso en el que se puedan ver afectados por el *outsourcing*.

Por otra parte, para conseguir ser lo más eficiente ante los riesgos es necesario que las entidades financieras sean lo más resilientes posibles ya que de esta manera serán capaces de poder hacer frente a los riesgos o incluso eludirlos y continuar con el funcionamiento ordinario.

PALABRAS CLAVE

Resiliencia operativa - Datos personales - Proceso de externalización - Clientes - Entidad financiera - Autoridad reguladora y supervisora - Riesgos no financieros.

ABSTRACT

In the financial sector, financial institutions may outsource some of their functions or activities to a service provider. This process is commonly known as outsourcing.

When financial institutions decide to outsource an activity, it is possible that they will face different potential risks. In this case, the so-called non-financial risks are analyzed, which are not related to financial management, but which can affect the operation of the financial institution in the same way.

The analysis has focused on the comparison of the regulation of personal data in the outsourcing process in three different areas: Europe, the United States and the United Kingdom. The regulatory and supervisory authorities of each area analyzed issue guidelines for all financial institutions in that area on how the outsourcing process should be carried out, and in particular, how the personal data of the financial institution's customers should be regulated and protected in the event that they may be affected by outsourcing.

On the other hand, in order to be as efficient as possible in the face of risks, it is necessary for financial institutions to be as resilient as possible, as in this way they will be able to cope with the risks or even avoid them and continue with normal operations.

KEY WORDS

Operational resilience – Personal data – Outsourcing – Clients – Financial institution – Regulatory and supervisory authority - non-financial risks

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO DE ABREVIATURAS

EBA	*European Bank Authority*
OCC	*Office of the Comptroller of the Currency*
UE	Unión Europea
DORA	Reglamente sobre Resiliencia Operativa Digital
IME	Instituto Monetario Europeo
ANC	Autoridades Nacionales Competentes
TIC	Tecnologías de Información y Comunicación
AES	Autoridades Europeas de Supervisión
RGPD	Reglamento General de Protección de Datos
ECPA	Ley de Privacidad de las Comunicaciones Electrónicas
GLBA	Ley de Privacidad de la Información Financiera del Consumidor
FTC	*Federal Trade Commission*
COPPA	Ley de Protección al Consumidor de Servicios de Información
FCRA	Ley de Informes de Crédito Justo
CPA	Ley de Privacidad del Consumidor de California
VCDPA	Ley de Privacidad del Consumidor de Virginia
APEC	Foro de cooperación económica Asia-Pacífico
CBPR	Sistema de Reglas de Privacidad Transfronteriza
DPA	*Data Protection Act*

CAPÍTULO I. INTRODUCCIÓN

1. CONTEXTO HISTÓRICO

A lo largo de la historia, el sector financiero se ha centrado más en la regulación y supervisión de los riesgos financieros como son el riesgo de mercado, el riesgo operativo o el riesgo de crédito, los cuales tienen un efecto sistémico y directo en la actividad del sector pudiendo causar un daño relevante en los mercados si no son controlados adecuadamente.[1]

Sin embargo, durante los últimos años se ha producido una importante incorporación de las nuevas tecnologías al sector financiero ya que han avanzado a un ritmo acelerado y, unido a los bajos tipos de interés que han imperado en el pasado reciente se han elaborado unos modelos de negocios que se caracterizan por estar digitalizados y automatizados. Como consecuencia de la mejora de la eficiencia y la velocidad de todos los procesos, han surgido nuevos riesgos que son los llamados riesgos no financieros. (European Banking Authority, 2019)

Dichos riesgos no financieros, aunque, como su propio nombre indica, no son financieros, afectan de la misma forma al sector bancario. Algunos ejemplos de riesgos no financieros pueden ser la ciberseguridad, a la protección de datos, al riesgo operacional o estratégico… (PWC, 2018)

Por otra parte, ha surgido la necesidad de adaptar la regulación o elaborar nuevas normas que abarquen estos riesgos no financieros que antes no se tenían en cuenta. Por ende, la regulación de los riesgos no financieros es menor pudiendo ocasionar unos daños relevantes e irreversibles.

Por ello, las distintas autoridades que regulan el sector financiero han tomado las medidas necesarias para que estos riesgos no financieros cuenten con unas normas y directrices propias, y para que tengan su regulación y estén supervisados, y todo ello con el fin de que las entidades financieras puedan identificar, evaluar y mitigar estos riesgos.

Además, debido a la creciente complejidad e interdependencia de los mercados financieros globales, las autoridades están estableciendo unos marcos regulatorios a nivel

[1] PWC. (2018). Los riesgos no financieros, una amenaza creciente para la banca. *PWC* https://ideas.pwc.es/archivos/20180302/los-riesgos-no-financieros-una-amenaza-creciente-para-la-banca/

global para hacer frente a esta nueva realidad y, además, dar la protección necesaria tanto a las entidades como a los usuarios involucrados en la comercialización de productos financieros. El objetivo primordial de la regulación global de estos riesgos no financieros es mejorar la resiliencia operativa del ámbito financiero.

La resiliencia operativa se define como la capacidad que tiene una entidad financiera parar continuar realizando sus funciones y actividades frente a alguna disrupción repentina. Esta capacidad permite al banco identificar y protegerse de distintos fallos y amenazas potenciales. Además, debe ayudar a las entidades financieras a adaptarse, recuperarse y aprender de estos eventos perturbadores para reducir el impacto futuro en sus funciones. (Financial Stability Institute , 2021)

2. OBJETIVOS

El objetivo del presente Trabajo de Fin de Grado consiste en el análisis de los riesgos no financieros que se pueden generar cuando las entidades financieras deciden realizar algunas de sus actividades a través de unos proveedores de servicios, lo que se conoce como externalización u *outsourcing.* En concreto, este trabajo se enfoca en el análisis de la protección de los datos personales. Además, se va a realizar una comparativa de la regulación en tres zonas distintas — Europa, Reino Unido y Estados Unidos — para poder obtener conclusiones del nivel de desarrollo normativo y protección que cuenta cada zona sobre los datos personales de sus ciudadanos.

Para llevar a cabo este trabajo se realiza, por un lado, un estudio de las regulaciones sobre la protección de datos que cuenta cada zona y, por otro lado, se realiza un análisis de la normativa que establecen y exigen las autoridades reguladoras y supervisoras — Autoridad Bancaria Europea, Oficina del Controlador de la Moneda en Estados Unidos y la Autoridad Prudencial Regulatoria en Reino Unido — a las entidades financieras de sus respectivas zonas sobre cómo se protege y se regula la protección de los datos de sus clientes cuando la entidad financiera externaliza actividades mediante la contratación con proveedores de servicios.

3. METODOLOGÍA

La metodología usada para la realización del presente Trabajo de Fin de Grado consiste en la realización de un análisis cualitativo de las diferentes regulaciones normativas sobre la relación de las entidades financieras con los proveedores de servicios en materia de *outsourcing*. En concreto, se analiza Europa, Estados Unidos y Reino Unido.

Una vez realizado el análisis y obtenido las conclusiones necesarias se llevará a cabo la elaboración de una tabla comparativa en la que se ilustren de manera descriptiva las diferencias y similitudes que se dan entre las distintas zonas analizadas.

CAPÍTULO II. MARCO TEÓRICO

1. EXTERNALIZACIÓN DE LAS ACTIVIDADES FINANCIERAS *(OUTSOURCING)*

1.1. Origen y evolución del *outsourcing*

El proceso de externalización de las actividades tiene su origen en Estados Unidos entorno a los años sesenta cuando las organizaciones consideraban necesario contratar diferentes servicios especializados en computación para que se les ayudase en la parte financiera de la organización.[2]

Las entidades financieras que realizaban procesos de externalización tenían unos indicadores de desempeño más elevados por lo que se vio un fuerte aumento de la competitividad y productividad en las entidades financieras que realizaban *outsourcing*. Por ende, el proceso de externalización de actividades comenzó a ser mucho más común.

Gracias a este proceso, las entidades financieras acceden con mayor facilidad a las nuevas tecnologías y consiguen llegar a tener economías de escala mediante la centralización de las funciones. (European Banking Authority, 2019)

Según la Autoridad Bancaria Europea, en inglés European Bank Authority (en adelante, "**EBA**"), durante los últimos cinco años las entidades financieras han mostrado un mayor interés por la externalización de las actividades especialmente por dos motivos principales.

Un primer motivo es la reducción de los costes que se produce y el aumento de la flexibilidad y eficiencia. Además, se da la posibilidad de que las entidades financieras puedan realizar actividades de las que no tienen conocimiento.

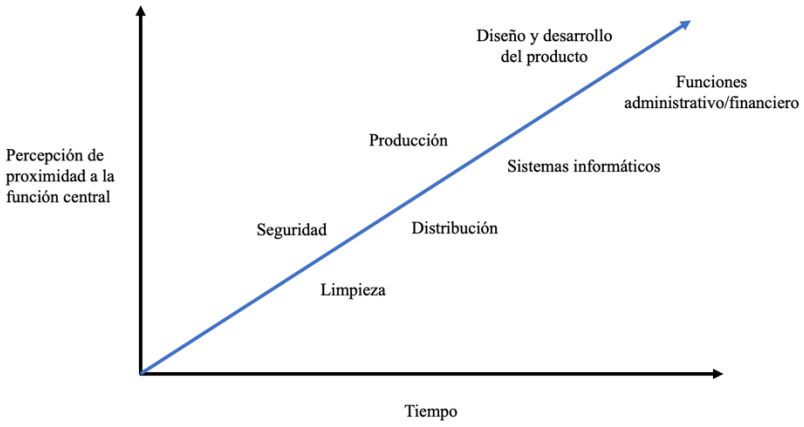
---

[2] Herrera Vinicio. G. (2019). Outsourcing. Conceptos fundamentales. *Gestiopolis*. https://www.gestiopolis.com/outsourcing-conceptos-fundamentales/

Un segundo motivo es, en el contexto de la digitalización, la creciente importancia de los nuevos proveedores de la tecnología financiera ("Fintech")[3], donde las entidades financieras deben de adaptar sus modelos de negocio para implementar dichas tecnologías.

Por otra parte, el *outsourcing* ha ido evolucionando y con ello las actividades que han ido utilizando este proceso. Primero se empezó con la externalización de actividades simples como puede ser la seguridad o el servicio de limpieza. Más tarde comenzó la subcontratación de actividades en las que la relación con el tercero debía de ser mucho más estrecha e interrelacionada como puede ser la distribución. Por último, estarían las entidades que ofrecen diferentes servicios a sus clientes como si fuese una única estructura, aunque realmente hay terceros involucrados. (López, 1999)

FIGURA 1: La evolución del outsourcing



FUENTE: Elaboración propia

1.2. Concepto

El término *outsourcing* es definido como el conjunto de actividades y de procesos que son tanto realizados como administrados por una empresa externa. (Werther & Davis, 2008). Si bien es cierto, el servicio suele ser definido durante un periodo específico de tiempo y a un precio acordado el cual suele ser limitado. (Heywood, 2002)

[3] La Comisión Nacional del Mercado de Valores define este término como "aquellas actividades que impliquen el empleo de la innovación y los desarrollos tecnológicos para el diseño, oferta y prestación de productos y servicios financieros".

Otra aproximación del término es "la subcontratación de servicios que busca agilizar y economizar los procesos productivos para el cumplimiento eficiente de los objetos sociales de las instituciones, de modo que las empresas se centren en lo que les es propio".[4]

El objetivo de la externalización es la concentración de los esfuerzos en las actividades principales del negocio mediante la delegación de las actividades complementarias a terceros. Como consecuencia, los clientes van a obtener un valor añadido ya que van a notar una agilidad y habilidad en los servicios que contratan. Además, las entidades financieras obtendrán una reducción de costes, de personal y de los tiempos en realizar los procesos. (Antonio Romero, 2002)

Por otra parte, la estructura de la entidad financiera no varía en el sentido de que el órgano de dirección sigue siendo el responsable de la entidad y de la vigilancia de todas las actividades. Para ello, se debe garantizar que la entidad financiera cuenta con todos los recursos necesarios para que el desempeño de las actividades propias de la entidad financiera se desempeñe adecuadamente. Además, se debe llevar a cabo la supervisión de todos los riesgos y la gestión de los acuerdos de externalización, no pudiendo dar lugar a una delegación de las responsabilidades. (European Banking Authority, 2019)

1.3. El riesgo *outsourcing*

El proceso de *outsourcing* lleva consigo unos riesgos. Esto se debe a que, aunque las entidades financieras decidan externalizar alguna actividad, deben ser conscientes de que siguen siendo responsables de cualquier incidente que pueda generarse de externalizar una actividad. Es decir, *outsourcing* no es sinónimo de estar exento de responsabilidad.[5]

Por ende, las entidades financieras seguirán siendo responsables de los fallos que cometan los terceros ante las autoridades reguladoras y supervisoras bancarias y todo ello con la finalidad última de proteger al cliente.

Por otra parte, externalizar ciertos procesos o funciones en una entidad financiera puede generar unos riesgos que pueden dar lugar a una pérdida del control tanto del proceso como del resultado esperado, además de la pérdida de la confianza por parte de los

[4] Romero A. (2002). Outsourcing. Qué es y cómo se aplica. *Gestiopolis.* https://www.gestiopolis.com/outsourcing-que-es-y-como-se-aplica/

[5] LASARTE, M. (2018). La externalización de la banca, bajo la lupa del BCE. *KPMG Tendencias.* https://www.tendencias.kpmg.es/2018/06/externalizacion-banca-bce/

clientes debido a la baja calidad de los resultados entregados e incluso por los retrasos de los plazos de entrega y todo ello conlleva unos costes imprevistos para la entidad financiera.

Para intentar mitigar los riesgos, las entidades financieras deben elaborar una estrategia de externalización centralizada alineada al mismo tiempo con la estrategia de negocio de la entidad a corto, medio y largo plazo. Una estrategia bien centralizada genera muchas oportunidades mientras que una no centralizada puede ocasionar unos riesgos en la entidad que quizás ni la entidad financiera era consciente de ellos. (Lasarte, 2018)

Por último, el *outsourcing* cuenta con ventajas y desventajas. Por un lado, la ventaja principal de externalizar procesos es que el coste de manufactura es menor. Otra ventaja es la aportación de innovación que puede generar el proveedor de servicios que a veces la propia entidad financiera no puede aportar. Por otro lado, la desventaja principal es la pérdida de control y de conocimiento ya que ambos residen en el *outsourcer*. No obstante, los resultados positivos suelen superar a los negativos teniendo el proceso de externalización un impacto positivo en las entidades financieras.[6]

2. RIESGOS NO FINANCIEROS

El riesgo financiero se define como "la posibilidad de que ocurran sucesos futuros, inciertos e independientes de la voluntad de quien lo sufre, susceptibles de ocasionar un perjuicio económico".[7]

Dicho riesgo surge de "las transacciones que realiza una empresa y que implican la utilización de derechos de cobro y obligaciones de pago". (EALDE, 2020) También es posible que se derive de las operaciones realizadas en los mercados financieros.

Por otra parte, en los últimos años, ha ido incrementando la presencia de un nuevo tipo de riesgo que amenaza a las entidades financieras. Dicho riesgo es el no financiero que, como su propio nombre indica, no tiene relación directa con la gestión financiera de la empresa, sino que proceden de factores internos y externos, pero que afecta tanto al

[6] Mendoza Zuleyma, E. (2015). Principales riesgos al contratar servicios de outsourcing. *Gestiopolis*. https://www.gestiopolis.com/principales-riesgos-al-contratar-servicios-de-outsourcing/

[7] Riveros, A. (2020). Introducción a la gestión de riesgos no financieros. *EALDE Business School.* https://www.ealde.es/gestion-de-riesgos-financieros/

funcionamiento de la empresa como a su éxito y por lo que deben de estar regulados y supervisados.

El análisis realizado se centra en un tipo específico de riesgo no financiero el cual va dirigido a la protección de datos. Si bien es cierto que existen otros tipos de riesgos no financieros que serán también analizados como son el riesgo operacional, reputacional, estratégico, de ciberseguridad.

2.1. Riesgo reputacional

Este riesgo no financiero es definido como la probabilidad que tiene una empresa u organización de que sufra una pérdida en su reputación, es decir, en la visión que tiene la sociedad sobre esa entidad. Como consecuencia, se produce una disminución del valor de la empresa.

Este riesgo no financiero cada vez es más relevante debido a que la sensibilidad social está creciendo y, además, existe una rápida transmisión de la información por el auge de las nuevas tecnologías.[8]

Dicho riesgo se caracteriza por su impacto transversal en toda la entidad financiera, es decir, en el momento en el que el riesgo reputacional está presente, toda la compañía va a verse afectada y, por consiguiente, se tendrá una reducción de valor. Es decir, no cabe que el riesgo reputacional afecte sólo a una parte de la entidad financiera.[9]

El riesgo reputacional, además de ser transversal, cuenta con dos características relevantes. La primera es que se considera un riesgo estratégico debido a que su consecuencia más común es la necesidad de desarrollar una estrategia por parte de la empresa para poder desenvolverse de una manera correcta ante el efecto producido. La segunda es que, aunque parece que no se puede cuantificar las pérdidas que conlleva este tipo de riesgo no financiero, sí que son medibles sus efectos. Por ejemplo, pueden acarrearse pérdidas en la empresa y éstas ser cuantificables por la empresa.[10]

---

[8] KPMG. (2023). La singularidad del riesgo reputacional. *KPMG Tendencias.* https://www.tendencias.kpmg.es/digitalizacion-gestion-riesgos-risk-analytics/la-singularidad-del-riesgo-reputacional/

[9] Riveros, A. (2020). Que son los riesgos no financieros y cómo afectan a las empresas. *EALDE Business School*. https://www.ealde.es/riesgos-no-financieros

[10] Riveros, A. (2021). Cómo gestionar y mitigar el riesgo reputacional en las organizaciones. *EALDE Business School.* https://www.ealde.es/gestion-de-riesgos-reputacional/

Por otra parte, existen dos tipos de riesgos reputacionales, por un lado, está el que se considera "puro" el cual va asociado directamente a problemas de confianza con los clientes, de transparencia, de conductas de la empresa dirigidas a la sociedad… Por otro lado, está el llamado "operacional", que tiene origen en algún problema de las operaciones y, por consiguiente, produce un mal funcionamiento de los procesos de la compañía afectando a la vez a la reputación de la entidad financiera. Por ejemplo, cuando un banco sufre pérdidas y tiene que ser ayudado por otra compañía, lleva como consecuencia el quebranto de su reputación.[11]

2.2. Riesgo estratégico o de negocio

Este riesgo no financiero es producido por una decisión de negocio fallida[12]. Es decir, los negocios están en constante contacto con este riesgo ya que la toma de cualquier decisión por parte de la entidad financiera puede producir un riesgo estratégico.

Normalmente, cuando se hace referencia al término "riesgo" se percibe por la sociedad como algo a evitar o a reducir. Sin embargo, no siempre tiene que conllevar el concepto "riesgo" una connotación negativa, sino que a veces ayuda a la institución a conseguir crear valor. Es decir, si el riesgo estratégico es enfocado de una manera correcta puede contribuir al buen desempeño del negocio. (Owen Ryan, 2016)

En la misma línea, las empresas que traten de proteger su valor ignorando a los disruptores seguramente se queden atrás, mientras que las empresas que anticipen los riesgos estratégicos pueden mejorar su rendimiento al aprovechar las oportunidades que presenten estos cambios.

Las sociedades que, hoy en día, son líderes, son aquellas que han logrado mantener su valor gestionando el riesgo. En un futuro, serán aquellas que consigan ver que del riesgo también se puede crear valor. (Owen Ryan, 2016)

[11] Riveros, A. (2021). Cómo gestionar y mitigar el riesgo reputacional en las organizaciones. *EALDE Business School.* https://www.ealde.es/gestion-de-riesgos-reputacional/

[12] Escuela Europea de Excelencia. (2022). Qué son los riesgos estratégicos y como abordarlos de forma eficaz. https://www.escuelaeuropeaexcelencia.com/2022/06/que-son-los-riesgos-estrategicos-y-como-abordarlos-de-forma-eficaz/

2.3. Riesgo tecnológico

El riesgo tecnológico se origina por el aumento de las tecnologías y nuevas herramientas que a veces no cuentan con unos estándares reconocidos internacionalmente y, además, las entidades financieras, en ocasiones, no los cumplen con rigor.

Existen diferentes tipos de riesgo tecnológico que son: (i) el riesgo digital que proviene de los sistemas software, (ii) el riesgo mecánico que se deriva del uso de herramientas, (iii) el riesgo químico que proviene del uso de sustancias químicas y el cual puede llegar a ser letal, (iv) el riesgo físico que proviene de los cálculos que toda máquina lleva detrás y un mínimo fallo en la exactitud puede desencadenar en un riesgo tecnológico, y (v) el riesgo biológico que engloba todos los riesgos que pueden producirse de utilizar las tecnologías en el sector biológico.[13]

Por ello, es esencial que las empresas cuenten con unas estrategias de negocio y de prevención de riesgo para adelantarse a los riesgos y de esta manera, no se llegue a interrumpir el correcto funcionamiento del negocio.

2.3.1. Ciberseguridad

La ciberseguridad se regula como un tipo de riesgo tecnológico.[14] Es definida como la práctica dirigida a la protección de todos los procesos y sistemas de la empresa y, en concreto, a la protección de la información confidencial que tiene recogida la empresa.[15]

El principal objetivo que tiene la ciberseguridad es conseguir que la entidad financiera tenga un correcto funcionamiento y que la infraestructura digital con la que cuenta esté regulada y protegida adecuadamente. [16]

Por otro parte, la ciberseguridad cuenta con un proceso de tres fases[17]. A continuación, se desarrollan las tres fases:

---

[13] Llamas, J. (2020). Riesgo Tecnológico. *Economipedia*. https://economipedia.com/definiciones/riesgo-tecnologico.html

[14] Ekon. (2021). Cómo analizar y gestionar el riesgo tecnológico empresarial. https://www.ekon.es/blog/riesgo-tecnologico-empresarial/

[15] Universae. (2022). Qué es la ciberseguridad. https://universae.com/blog/que-es-ciberseguridad/

[16] Universidad Europea. (2022). ¿Qué es la ciberseguridad? *Universidad Europea.* https://universidadeuropea.com/blog/que-es-ciberseguridad/

[17] International Online Education. Cuáles son las fases de la ciberseguridad. *International Online Education*. https://www.euroinnova.edu.es/cuales-son-las-fases-de-la-ciberseguridad

- La fase de prevención consiste en la elevación del nivel de conciencia por parte de la entidad financiera para la visualización de las amenazas a las que se está expuesto. De la misma manera que todos los riesgos anteriores mencionados, es esencial que exista una adecuada prevención de riesgos, sea cual sea el tipo, para conseguir que el funcionamiento de la empresa no se interrumpa.
- La fase de localización se basa en el deber de las empresas de conocer los puntos de vulnerabilidad para conseguir la eliminación de cualquier riesgo de entrada.
- La fase de reacción consiste en el deber de la empresa de desarrollar y tener en acción un plan de contingencia para disminuir las posibles amenazas y, en el caso de que se produjese una amenaza reducir las consecuencias más graves. Un plan de contingencia engloba todas las medidas que desarrolla una empresa para desenvolverse de la mejor manera en una situación extraordinaria y así asegurar un correcto funcionamiento y una continuidad del negocio.

2.4. Riesgo operacional

El gobierno británico menciona la siguiente frase "mantengan la calma y sigan adelante". Quería hacer referencia a esta expresión por la relación que tiene con este tipo de riesgo ya que el fundamento básico de este riesgo es la capacidad de la empresa para seguir operando bajo cualquier suceso inesperado.

El riesgo operacional es definido como toda contingencia que pueda provocar posibles pérdidas en la empresa a causa de conductas humanas inadecuadas, errores tecnológicos, por factores externos o procesos internos defectuosos. Es por ello, que la expresión mencionada se acuñó con la intención de motivar a las entidades financieras a perseverar frente al desafío. (Banco de Inglaterra, 2019)

La resiliencia operativa procede de este tipo de riesgo y es definida como la capacidad de las empresas para seguir prestando el servicio financiero.

Por otra parte, se establece que las entidades financieras *"*deben considerar la cadena de actividades que componen un servicio de negocios, desde que se asume la obligación hasta que se cumple con el servicio, y determinar qué parte de la cadena es crítica para el cumplimiento*".* (Banco de Inglaterra, 2019)

Una vez determinada, la empresa debe centrarse en esos puntos críticos y desarrollar un plan de mitigación para eliminar o disminuir el riesgo de incumplimiento del servicio prestado. (Consejo de la Unión Europea, 2022)

Este riesgo se aumenta con la externalización de las actividades a terceros ya que la prestación del servicio depende de una cadena más compleja provocando un aumento de los riesgos sobre la resiliencia operativa.

En definitiva, con la resiliencia operativa se consigue evaluar y documentar la capacidad que posee la entidad financiera para continuar operando su servicio en el caso de que un riesgo adverso se concrete por no haber podido eludirlo.[18]

2.4.1. Reglamento sobre la Resiliencia Operativa Digital

Después de la crisis financiera del 2008, las autoridades reguladoras vieron la necesidad de que las instituciones financieras, además de que mantuviesen una liquidez apta para hacer frente a las pérdidas sufridas, continuasen con un rendimiento de trabajo elevado para que el sistema financiero no se viese desestabilizado. (Kelly, 2020)

Por otro parte, el auge de las nuevas tecnologías ha incidido y revolucionado el sector financiero de manera que las entidades financieras se han visto obligadas a adaptar los modelos de negocio y desarrollar unos más competitivos. Por ello, resulta esencial que todo el sistema tecnológico funcione de una forma adecuada para que la resiliencia operativa quede garantizada.

La Unión Europea (en adelante, "**UE**") decidió reforzar la seguridad de todas las entidades financieras como pueden ser los bancos o las empresas de inversión debido al aumento de los ciberataques y, es por ello, que el Consejo Europeo desarrolla el Reglamento sobre la resiliencia operativa digital (en adelante, "**Reglamento DORA**") que garantiza que el sector financiero actúe de forma resiliente cuando se produzca una ardua perturbación operativa. (Consejo de la Unión Europea, 2022)

Fue en el año 2020, cuando la Comisión presentó el Reglamento DORA como parte de un proyecto en el que se recoge un amplio abanico de medidas de finanzas digitales con el objetivo de fomentar el desarrollo tecnológico, garantizar la estabilidad financiera y la protección de los consumidores. Como parte del proyecto, también se incluía (i) una estrategia sobre las finanzas digitales, (ii) una propuesta sobre los mercados de criptoactivos, y (iii) una propuesta sobre la tecnología de registro descentralizado. En definitiva, el objetivo del Reglamento DORA es apoyar la innovación y la adopción de

[18] Pérez. Y. Poniendo foco en la resiliencia operativa. *KPMG Tendencias*. https://www.tendencias.kpmg.es/2021/03/poniendo-foco-en-la-resiliencia-operativa/

nuevas tecnologías financieras, aportando a la vez una adecuada protección para los consumidores y los inversores. (Consejo de la Unión Europea, 2022)

El propósito de todo el proyecto era llenar un vacío legal en la legislación de la UE al asegurar que el nuevo marco jurídico regulatorio no obstaculizara el uso de nuevos instrumentos financieros digitales, y a la vez se garantizase que estas nuevas tecnologías y productos estuvieran sujetos a los mecanismos de regulación y gestión de riesgos operativos del sector financiero de las empresas activas en la UE. (Consejo de la Unión Europea, 2022)

Gracias al Reglamento Dora se consigue una armonización del régimen legal de los requisitos legales del sector financiero para garantizar que el sector esté operativo en todo momento y actúe con mayor eficiencia. (Stanjura, 2022) Es decir, se establecen unos requisitos homogeneizados para todos los Estados Miembros de la UE e impone a todas las entidades financieras la capacidad de poder eludir o resistir a cualquier riesgo o amenaza relacionado con las tecnologías de información y comunicación (en adelante, "**TIC**").

Por otra parte, cuando el Reglamento DORA se aprobó y entró en vigor, cada Estado Miembro de la UE tuvo que incorporarlo a su legislación y las distintas Autoridades Europeas de Supervisión (en adelante, "**AES**"), como puede ser la Autoridad Bancaria Europea, mencionada anteriormente, deberán desarrollar sus propias normas técnicas conforme al Reglamento Dora y, por ende, las entidades financieras deberán de cumplir con todo el desarrollo normativo.

Por último, el artículo 3 del Reglamento DORA define el término resiliencia como "la capacidad de una entidad financiera para construir, asegurar y revisar su integridad y fiabilidad operativas asegurando, directa o indirectamente mediante el uso de servicios prestados por proveedores terceros de servicios de TIC, toda la gama de capacidades relacionadas con las TIC necesarias para preservar la seguridad de las redes y los sistemas de información que utiliza una entidad financiera y que sustentan la prestación continuada de servicios financieros y su calidad, incluso en caso de perturbaciones". (Consejo de la Unión Europea, 2022)

3. AUTORIDADES REGULADODAS Y SUPERVISORAS

En algunas situaciones, como se ha mencionado en epígrafes anteriores, los sistemas financieros pueden fallar o incurrir en riesgos que afecten a los clientes finales. Por ello,

con la necesidad de evitar situaciones problemáticas y que se produzca una pérdida de confianza por parte de los clientes surgen las autoridades reguladoras y es de la forma en la que los estados pueden intervenir para regular y supervisar el sector financiero.

Existe una elevada heterogeneidad en las formas en las que las autoridades regulan y vigilan la externalización.

A continuación, se realiza un análisis de las respectivas autoridades reguladoras y supervisoras en Europa, Estados Unidos y Reino Unido.

3.1. Europa

En Europa, el Banco Central Europeo fue creado el 1 de junio de 1998 con sede en Alemania y se configura como el banco central de los 19 países de la UE que han adoptado como moneda única el euro.

Surgió con la finalidad de llevar a cabo los proyectos preparados por el Instituto Monetario Europeo (en adelante, "**IME**") que, en concreto, son: (i) la aplicación de la disciplina presupuestaria y (ii) mejorar la convergencia de todas las políticas monetarias y económicas de los 19 estados miembros de la UE.[19]

Entre las funciones principales se encuentran, por un lado, mantener la estabilidad financiera de los precios de toda la zona euro, ayudando así al crecimiento económico y, por otro lado, mejorar la vida de los ciudadanos. Además, define y ejecuta la política monetaria, también asegura que hay una aplicación correcta de todos los reglamentos y normativas en materia de supervisión y, es el encargado de supervisar todos los bancos que están incluidos en la zona euro y todo ello con el fin último de proteger a los consumidores. (Banco Central Europeo, 2023)

Por otra parte, en el año 2014 se funda el Mecanismo Único de Supervisión integrado por el Banco Central Europeo y las demás Autoridades Nacionales Competentes (en adelante, "**ANC**") que pertenecen a los estados miembros de la UE. Se constituye como el mecanismo a través del cual se realiza la función de supervisión de la estabilidad financiera.

[19] Banco de España. Las tres fases de UEM. https://www.bde.es/wbe/es/sobre-banco/actividad-europea/eurosistema-sebc/historia-eurosistema/uem/fases-uem/

En definitiva, EBA mantiene una estrecha relación con los restantes bancos nacionales y otros organismos de la UE para conseguir que la política monetaria sea eficaz y coherente. (Banco Central Europeo, 2023)

La manera en la que cooperan el Banco Central Europeo y las autoridades nacionales competentes es a través del *Joint Supervisory Teams* (en adelante, "**JST**"). Se configura como un equipo de investigación conjunto y cuya función es la supervisión del cumplimiento de la normativa por parte de los bancos más importantes con los mismos fines de siempre que son: (i) garantizar la estabilidad financiera y (ii) proteger al consumidor en todo momento. Además, supervisa que los bancos tengan controlada la gestión de los riesgos. (European Central Bank, 2023)

3.2. Estados Unidos

La autoridad reguladora y supervisora de Estados Unidos es la Oficina del Controlador de la moneda, siendo la traducción en inglés *Office of the Comptroller of the Currency.* (Office of the Comptroller of the currency, s.f.)

El 25 de febrero de 1863, el presidente Lincoln promulgó la Ley de la Moneda Nacional *(National Currency Act)*. Esta ley fue la base para la creación de la Oficina del Controlador de la Moneda (en adelante, "OCC"), encargada de organizar y administrar un sistema de bancos nacionales y una moneda nacional uniforme. Por ende, gracias a esa ley se creó la OCC como una oficina independiente del Departamento del Tesoro de Estados Unidos.

La OCC lleva a cabo su misión realizando las siguientes tareas:

- Se encarga de autorizar, regular y supervisar todos los bancos nacionales, las asociaciones federales de ahorro y las sucursales y agencias federales de bancos extranjeros, y además de la supervisión de que operen de forma segura.
- Proporcionar un acceso equitativo a los servicios financieros, que éstos traten a los clientes de forma justa y cumplan las leyes y reglamentos aplicables.
- Imponer medidas correctivas, cuando sea necesario, a los bancos gobernados por la OCC que no cumplan las leyes y reglamentos o que incurran en prácticas inseguras o poco sólidas.
- Proteger a los consumidores asegurándose de que los bancos ofrezcan un acceso justo y un trato equitativo a los clientes y cumplan la legislación en materia de banca de consumo

Por otra parte, la OCC cuenta con que los bancos tengan unos procesos de gestión de riesgos coherentes y proporcionales al nivel de riesgo y complejidad de sus relaciones con terceros y a las estructuras organizativas del propio banco. Por lo tanto, la OCC realizará una supervisión y una gestión más exhaustiva y rigurosa de las relaciones con terceros que impliquen actividades críticas o servicios compartidos problemáticos (tecnología de la información), u otras actividades que impliquen un riesgo considerable para el banco.

3.3. Reino Unido

El Banco de Inglaterra es el encargado de la regulación y supervisión de las empresas de servicios financieros a través de la Autoridad de Regulación Prudencial (sus siglas en inglés son, *Prudential Authority Regulation*). Esta autoridad fue creada en la nueva oleada de regulación de los servicios financieros tras la crisis financiera de 2007. (Bank of England, 2023)

Esta autoridad se constituye como una autoridad reguladora prudencial. Esto se caracteriza por ser una autoridad que, por un lado, se encarga de crear políticas para que las empresas las lleven a cabo y, por otro lado, vigila el funcionamiento de las empresas por lo que también tienen la función de supervisar. Se quiere garantizar que los servicios y productos financieros de los que todos dependen se presten de forma segura y sólida.

Para cumplir con los objetivos, el Banco de Inglaterra toma las siguientes medidas:

- Se realiza una supervisión a medida, es decir, se caracteriza por ser un proceso especializado y cada empresa es supervisada en función de sus necesidades y del impacto que tendría en la economía en caso de quiebra. Como consecuencia de esta supervisión, se permite que se detecten los fallos a tiempo.
- La supervisión va dirigida hacia el futuro. Si bien es cierto, las entidades financieras pueden funcionar correctamente hoy en día, pero ¿qué puede producirse en la entidad ante un suceso incierto? Para reducir la producción de unas consecuencias destructivas en la entidad, la autoridad se encarga de elaborar diferentes escenarios para comprobar cómo las entidades financieras responderían a esos sucesos. Gracias a ello, se les ayuda a elaborar estrategias para poder resistir a esas situaciones de crisis.
- Por último, la autoridad realiza una visión de conjunto, es decir, proporciona la existencia de una garantía de que todo el sector financiero funciona de forma

correcta y sólida. Es decir, se ocupa de todo el sector en conjunto. Y así, en caso de que ocurra algún acontecimiento adverso, se intentará garantizar que ocurra de forma ordenada.

CAPÍTULO III. LA REGULACIÓN DE LA PROTECCIÓN DE DATOS EN DISTINTAS REGIONES DEL MUNDO

1. EUROPA

El desarrollo normativo de la UE referente a la protección de datos siempre ha sido de gran relevancia. En los últimos 25 años, el mundo se ha visto afectado por el auge de las nuevas tecnologías que ha conllevado a la necesaria revisión de las normas de protección de datos.

En el año 2016, la UE adoptó el Reglamento General de Protección de Datos (en adelante, "**RGPD**"), el cual se considera uno de sus mayores logros de los últimos años. Este reglamento va a derogar la Directiva de Protección de Datos de 1995 (Consejo de la Unión Europea, 1995) que fue desarrollada en una época en la que las nuevas tecnologías aún no estaban en auge y, por consiguiente, dicha directiva quedó insuficiente siendo necesaria la elaboración de una nueva normativa que regulase los nuevos aspectos. (Consejo de la Unión Europea, 2016)

El RGPD se reconoce como una ley de alcance general aplicable a todos los Estados Miembros de la UE. Después de su aprobación, todos los Estados Miembros disponían de un máximo de dos años para garantizar su plena aplicación en sus países, es decir, debía de estar implantado y en vigor antes del 25 de mayo de 2018.

Además de la aplicabilidad directa del RGPD en todos los Estados Miembros, éstos deberán adoptar ciertas regulaciones para asegurarse del cumplimiento de dicho reglamento dentro de sus fronteras.

1.1. Concepto

El reglamento define el término datos personales como toda la información sobre una persona física identificada o identificable mediante un identificador que suele usarse, entre otros, un nombre, un dato de localización o características de la identidad física, económica, cultural…

Los datos personales suelen ser procesados, es decir, el tratamiento de datos es un procedimiento común en las entidades financieras. Este término hace referencia al

conjunto de operaciones que se realizan respecto a los datos personales que pueden ser, entre otras, la recogida, el registro, la modificación, la difusión o la supresión o destrucción de los datos personales.

Para lo que incumbe en este análisis, es conveniente definir el concepto "tercero" como la persona física o jurídica — distinta al interesado o del responsable del tratamiento — que está autorizada para tratar los datos personales de un cliente.

1.2. Directrices

1.2.1. Principios generales y derechos del sujeto

Dentro del RGPD se establecen una serie de principios generales que debe de cumplir cualquier tipo de institución financiera respecto a los datos personales de sus clientes. Los dos principios más relevantes son:

- Principio de responsabilidad *("accountability")*: Las entidades financieras deben implementar diferentes tipos de mecanismos para asegurarse de que cumplen con todas sus obligaciones respecto a los datos personales. Se considera una responsabilidad proactiva.
- Principio de transparencia *("lawfulness, fairness and transparency"):* Las entidades financieras deberán adaptar unas políticas de privacidad en las que el cliente pueda entender adecuadamente el tratamiento de sus datos personales.

Si bien es cierto, existen otros principios básicos que las entidades financieras deben de tener en consideración como que la recopilación de datos personales debe tener un fin específico y deben recogerse sólo los adecuados o relevantes para la consecución de dicho fin. Además, que el almacenamiento de dichos datos sólo puede durar el tiempo necesario para dicho fin. Por último, las entidades financieras deben afirmar que el proceso se realiza de forma segura y que los datos de sus clientes están debidamente protegidos.

Por otra parte, el responsable del tratamiento de los datos personales debe proveer al cliente con toda la información sobre sus derechos de manera clara, concisa e inequívoca.

Se debe tener en consideración la diferencia entre responsable y encargado del tratamiento de datos. El responsable es la persona que se encarga de determinar tanto los fines como los medios que tienen relación con el tratamiento de datos mientras que el encargado es el que trata los datos personales según las indicaciones del responsable. En

ocasiones, los encargados pueden ser los proveedores de servicio con los que se contrata un proceso de externalización. (Comisión Europea, 2023)

Por último, algunos derechos que tienen los clientes sobre sus datos son:

- Derecho a obtener información sobre el tratamiento de sus datos personales y, por ende, acceder a ellos siempre que lo requiera. ("*Right of Access*")
- Derecho a solicitar cualquier modificación sobre sus datos personales sin ningún tipo de demora innecesaria. Además, el interesado puede presentar una declaración complementaria para asegurarse de que los datos sean precisos y completos. ("*Right to rectification*")
- Derecho a solicitar la eliminación de los datos personales si éstos ya no son necesarios para los propósitos para los cuales fueron recopilados. Es decir, el interesado puede solicitar que sus datos sean eliminados si ya no hay una justificación válida para su procesamiento. ("*Right to erasure*")
- Derecho a solicitar que se limite el procesamiento de sus datos personales en ciertas circunstancias específicas. Es decir, el interesado tiene el derecho a limitar el procesamiento de sus datos personales bajo ciertas condiciones. ("*Right to restriction of processing*")
- Derecho a oponerse al procesamiento de sus datos personales en ciertas circunstancias, como el procesamiento con fines de marketing directo. ("*Right to object*")
- Derecho a no ser objeto de una decisión automatizada — la elaboración de perfiles — que produzca efectos jurídicos en él o le afecte de una manera significativa. ("*Automated individual decision-making including profiling*")

1.2.2. Autoridades supervisoras independientes

El presente Reglamento expresa que cada Estado Miembro tiene el deber de establecer una o varias autoridades encargadas de revisar que el Estado Miembro cumple de manera adecuada con la aplicación de la normativa desarrollada en RGPD. El fin de este control es la protección de los derechos y libertades fundamentales de las personas en relación con el tratamiento de sus datos personales y, además, de facilitar la libre circulación de datos personales en la UE.

Por otra parte, se exige que cada Estado Miembro se asegure de que cada autoridad cuenta con unas infraestructuras adecuadas para el perfecto desarrollo de sus actividades y con los recursos humanos, técnicos y financieros necesarios.

Dentro de la UE, se exige que las autoridades de cada Estado Miembro cooperen entre sí facilitándose la información pertinente y prestándose asistencia con el objetivo principal de que el presente Reglamento se ejecute y aplique de la manera más coherente.

1.2.3. Responsabilidad de las autoridades y sanciones

Cada interesado tiene el derecho a presentar cualquier tipo de reclamación ante una autoridad de control que, en concreto, será la del Estado Miembro donde resida habitualmente, se encuentre su lugar de trabajo o el lugar donde se haya cometido la infracción a reclamar en materia de protección de sus datos personales. Este proceso trae causa del derecho a tener una tutela judicial efectiva.

Por ende, todas las personas que puedan ver o hayan visto violado el derecho de protección de sus datos personales, serán indemnizadas conforme a la normativa del presente Reglamento. Además, cada Estado Miembro puede determinar el régimen de sanciones respecto a las infracciones producidas de la inaplicación del Reglamento en dicho Estado.

2. ESTADOS UNIDOS

Como primer punto a establecer, Estados Unidos no cuenta con un marco normativo único que sea equivalente al Reglamento General de Protección de Datos que existe en Europa. Es decir, la protección de datos en Estados Unidos está regulada por un conjunto de leyes tanto federales como estatales.

Estados Unidos ofrece una amplia libertad a las empresas para la regulación de la protección de los datos y de privacidad a corto plazo. Si bien es cierto, a largo plazo se exige a las empresas que estén capacitadas para adaptarse a los cambios y las nuevas leyes que pueden entrar en vigor.

A continuación, se desarrollan algunas leyes existentes, a nivel federal, sobre la protección de datos:

- Ley de Privacidad de las Comunidades Electrónicas (en adelante, "**ECPA**"): Fue aprobada en 1986 por el Congreso de Estados Unidos. El objetivo de dicha ley es la regulación de la protección de todos los datos y registros que se generan por

medios electrónicos como pueden ser los correos electrónicos o las comunicaciones telefónicas y lo que se establece es la prohibición de interceptación no autorizada. Además, se regula la divulgación de los datos generados en comunicaciones electrónicas por parte de los proveedores de servicios. (Rumold, 2016)

- Ley de Privacidad de la Información Financiera del Consumidor (en adelante, "**GLBA**"): Esta ley, también llamada Ley Gramm- Leach-Bliley, fue aprobada en el año 1999. Dicha ley recoge los requisitos que deben de cumplir las entidades financieras cuando realizan intercambios de información de datos confidenciales de los clientes. Por otra parte, se exige que las entidades financieras informen a sus clientes sobre las políticas de privacidad y, además, se les ofrece a los clientes la opción de aceptar o no el traspaso de información a otros proveedores de servicios. (Comisión Federal del Comercio, 1999)

  En la misma línea, esta ley requiere que la *Federal Trade Commission* (en adelante, "**FTC**") y otras agencias que regulan las instituciones financieras implementen un desarrollo normativo para llevar a cabo todo el contenido exigido en dicha ley.
- Ley de Protección al Consumidor de Servicios de Información (en adelante, "**COPPA**"): Esta ley fue aprobada en el año 1998 con el fin de regular la información personal y el uso de ésta de niños menores de 13 años. En consonancia a esto, se regula que todas las empresas que tengan la sede en Estados Unidos se hagan cargo de que sus sitios web contengan en su política de privacidad la petición del consentimiento verificable de los padres o del tutor del menor antes de recopilar cualquier tipo de información personal. (Comisión Federal del Comercio)
- Ley de Informes de Crédito Justo [20] (en adelante, "**FCRA**"): Esta ley establece la regulación que se debe seguir para proteger la información de los consumidores, en especial, la información que tienen las agencias de información crediticia.[21]

Por otra parte, algunos estados han llevado a cabo la elaboración de sus propias leyes como puede ser en el caso del Estado de California que cuenta con la Ley de Privacidad

[20] Christina Spicer. (2020). ¿Qué es la Ley de Información Crediticia Equitativa? *Top Class Actions*. https://topclassactions.com/es/glossary/fair-credit-reporting-act/

[21] La información que tienen las agencias crediticias sobre una personal es confidencial. Dicha información puede relevar condiciones personales que sean controvertidas o sobre su capacidad económica.

del Consumidor de California (en adelante, "**CPA**") o la Ley de Privacidad del Consumidor de Virginia (en adelante, "**VCDPA**").

Por un lado, CPA es la primera ley completa sobre la protección de datos que entró en vigor el 1 de enero de 2020 y todos los derechos y obligaciones recogidos en la ley se pueden equiparar a los recogidos por el RGPD. Esta ley proporciona a todos los consumidores de California una amplia variedad de derechos sobre la privacidad de sus datos. Además, se establecen las obligaciones que deben de cumplir las empresas como pueden ser el acceso a los datos, la eliminación, la portabilidad… (Microsoft , 2023)

Por otro lado, al igual que la ley de California otorga derechos a sus consumidores, la VCDPA proporciona derechos a sus consumidores sobre la protección de sus datos personales por parte de empresas que operan en Virginia. Esta ley ha sido aplicada por el Fiscal de Virginia a partir del 1 de enero de 2023, es decir, es una ley reciente. (Microsoft, 2023)

Por último, Estado Unidos entró dentro del foro de cooperación económica Asia-Pacífico (en adelante, "**APEC**") en el año 1989. Dentro de este foro de cooperación se han establecido unas reglas de Privacidad Transfronteriza (en adelante, "**CBPR**") donde se establecen unos requisitos mínimos sobre la protección de los datos.

El sistema CBPR contiene un código de conducta de privacidad de datos el cual aplica a todas las empresas que operen dentro del APEC y además deberán de aprobar una evaluación continua realizada por agentes autentificados por la APEC. (Galvez, 2019)

El contenido de dicho código tiene su base en ocho principios de privacidad que se encuentran dentro del Marco de Privacidad del APEC que son: (i) información sobre el tratamiento, (ii) limitación de la recopilación, (iii) uso de los datos personales, (iv) libre elección, (v) integridad, (vi) salvaguardas de seguridad, (vii) acceso y corrección, (viii) y responsabilidad. (Galvez, 2019)

En definitiva, el CBPR que es desarrollado a partir del Marco de Privacidad de APEC "se constituye como un modelo de autorregulación adecuado que combina la rigurosidad de principios recogidos en los marcos normativos de protección de datos personales con los flujos transfronterizos de datos entre las economías de APEC". (Galvez, 2019)

3. REINO UNIDO

En Reino Unido se debe de hacer una distinción entre la época anterior al Brexit y la posterior. Cuando Reino Unido pertenecía a la UE se aplicaba el RGPD, en general, como

un país más de la UE. Sin embargo, con la salida del país de la UE se realiza una distinción entre la aplicación del RGPD y el *Data Protection Act* (en adelante, "**DPA**")

El DPA entró en vigor el 23 de mayo de 2018 y aplica a todos los ciudadanos ingleses mientras que RGPD aplica a aquellos ciudadanos europeos que residen en Reino Unido.

No obstante, aunque puedan parecer dos normativas independientes, realmente el DPA que aplica a los ingleses es un desarrollo normativo que complementa el RGPD que aplica a la UE.

3.1. Aspectos relevantes

El DPA regula y controla cómo se debe de proteger la información personal que es utilizada por organizaciones, negocios o incluso el mismo gobierno. (UK Government, s.f.)

En primer lugar, el DPA cuenta con las mismas definiciones que se establecen en el RGPD, es decir, el DPA se remite a este último. (UK Government, 2018)

Respecto a los principios generales, el mismo DPA establece al igual que el RGPD seis principios generales en los que se debe de basar todo procedimiento que incluya el uso de datos. Por ello, cualquier procedimiento en el cual se vean afectados datos debe de contar con las siguientes características para asegurar su protección:

- El uso de los datos deberá ser legal y justo.
- Cualquier recogida de datos deberá de hacerse de manera específica, explícita y legítima.
- Los datos que se recogen deben de ser coherentes con los fines para los que se coleccionan.
- Los datos deben de ser precisos, además de ser los necesarios.
- Los datos tienen que ser guardados por un tiempo limitado, es decir, no pueden ser recopilados por más tiempo del necesario.
- Los datos tienen que estar seguros. En este principio se incluye también la protección contra el tratamiento de datos no autorizado.

En suma, el DPA recoge también los derechos que tienen los sujetos que coinciden con los del RGPD.

Por otra parte, el artículo 109 del DPA establece que los datos personales de ciudadanos ingleses no podrán ser transferidos fuera de Reino Unido a menos que la transferencia sea

necesaria en consonancia con la ley de Servicios de Seguridad de 1989 o la Ley de Servicios de Inteligencia de 1994.

En definitiva, se puede observar como el DPA regula muchos aspectos de la misma manera que el RGPD. Esto tiene su fundamento en que cuanto más parecidos sean más beneficioso será para la libertad de transferencia de datos como se explicará en el apartado posterior.

3.2. Diferencias entre el RGPD y el DPA

Como se ha mencionado en el apartado anterior, este acto es una implementación del RGPD, es decir, su contenido es bastante similar incluyendo algunas diferencias (DPO Centre, 2018). A continuación, se exponen algunas diferencias:

- La primera diferencia que establecer es sobre la edad de los niños para que el consentimiento sea válido. En el RGPD la edad mínima son los 16 años mientras que la edad en el DPA son los 13 años.
- La diferencia en la toma de decisiones y tratamiento automatizados radica en que en el RGPD tienen el derecho a decidir si quieres que sus datos sean automatizados y procesados. Sin embargo, el DPA regula ese derecho siempre y cuando haya motivos legítimos. En concreto, este derecho se regula en los artículos 49 y 50 del DPA estableciendo que no se podrán tomar decisiones significativas basadas en decisiones automatizadas si afecta de una manera considera al sujeto o produce un efecto legal adverso sobre éste.
- Sobre los derechos del sujeto, el RGPD asegura que todos los sujetos tienen derechos sobre el procesamiento de sus datos personales mientras que el DPA permite que estos derechos no se tengan en cuenta en el caso de que su cumplimiento produjera en la organización un efecto grave no pudiendo la organización desempañar sus funciones cuando realice el tratamiento de datos con fines científicos, estadísticos o históricos.
- El RGPD ofrece a los Estados Miembros un margen para que puedan equilibrar el derecho a la intimidad de los datos personales con el derecho a la libertad de expresión y de información. Sin embargo, el DPA realiza alguna exención en algunos requisitos de protección de los datos personales en relación con datos personales que hayan sido tratados con intereses públicos.

Estas diferencias son importantes de establecer ya que los datos podían entrar y salir de Reino Unido fácilmente cuando Reino Unido era un Estado Miembro de la UE lo que conllevaba una simplificación de los negocios incluso una reducción de los costes y aumento de la rapidez.

Con la aprobación del Brexit, los datos no podrían ser transferidos libremente dentro de la UE y dependerá de si las leyes de protección de datos son adecuadas.[22] Con esto se quiere expresar que la UE confiará en la transferencia de los datos de sus ciudadanos con Reino Unido cuanto más similares sean las leyes de protección de datos de Reino Unido al RGPD. Por ello, las diferencias entre el RGPD Y DPA son importantes ya que cuanto más amplias sean las diferencias menos facilidades se proporcionarán para transferir datos entre la UE y Reino Unido.

TABLA 1: Comparativa de la regulación de la protección de datos

	EUROPA	**ESTADOS UNIDOS**	**REINO UNIDO**
Autoridad Supervisora	Autoridad Europea Bancaria	Oficina del Controlador de la Moneda	Autoridad de la Regulación Prudencial
Marco normativo	Marco Regulatorio único	Enfoque fragmentado	Dos normativas aplicables
Modo de regulación	Reglamento General de Protección de Datos	Leyes federales Leyes propias en algún Estado	Ciudadanos europeos en Reino Unido: RGPD Ciudadanos ingleses: DPA

FUENTE: Elaboración propia

[22] Concepto definido en el artículo 45 del RGPD.

CAPÍTULO IV. ANÁLISIS COMPARATIVO DEL PROCESO DE EXTERNALIZACIÓN EN MATERIA DE PROTECCIÓN DE DATOS.

En el epígrafe anterior, se ha desarrollado, en general, la normativa que regula la protección de los datos personales en Europa, Reino Unido y Estados Unidos. Sin embargo, en este apartado se va a mostrar como la Autoridad Bancaria Europea (siglas en inglés, EBA), la Oficina Controlador de la Moneda (siglas en inglés, OCC) y el Organismo Regulador Prudencial (siglas en inglés, PRA) establecen diferentes desarrollos normativos, en sus respectivos países, sobre cómo las entidades financieras deben regular la protección de los datos cuando realizan procesos de externalización con terceros.

De esta manera se obtendrá una visión comparada para establecer el nivel de firmeza o exigencia que tiene cada país para regular los riesgos que conlleva la externalización en materia de protección de datos.

1. *EUROPEAN BANK AUTHORITY*

En el ámbito de la Unión Europea, el proceso de externalización de las actividades u *outsourcing* se encuentra regulado en las directrices sobre la externalización de la Autoridad Bancaria Europea (EBA) que fueron emitidas el 25 de febrero del 2019.

La Autoridad Bancaria Europea vio la necesidad de introducir las directrices sobre la externalización para obtener un marco regulador más armonizado como consecuencia de (i) los recientes cambios en el desarrollo normativo del sector bancario, (ii) el incremento de los ataques de ciberseguridad y (iii) el auge de las nuevas tecnologías y su creciente incorporación a los modelos de negocio de las entidades financieras. (Banco Central Europeo, 2019)

1.1. Objeto de las directrices EBA

Las directrices de la EBA[23] definen el término *outsourcing* como el "acuerdo de cualquier forma entre una entidad, 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".[24] Dicho de otras palabras, consiste en la delegación de la actividad de una empresa a un proveedor de servicios.

[23] Directrices EBA, 25 de febrero de 2019, sobre Externalización (EBA/GL/2019/02)
[24] Directrices EBA, *Op. Cit*., artículo 12.

De la misma manera, las directrices definen el término 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".[25]

Estas directrices ponen especial énfasis en la protección de los riesgos que se generan por la contratación de servicios con terceros y, en concreto, respecto a la protección de los datos personales de los clientes.

En la misma línea, las directrices tienen por objeto la regulación y especificación de los sistemas de gobierno interno — incluido la gestión de diferentes riesgos — que deben de adoptar las entidades financieras a la hora de externalizar funciones esenciales debido a que los requisitos exigidos son más concretos y estrictos por el elevado riesgo que tiene el *outsourcing*. Además, desarrollan normativa sobre cómo deben las autoridades competentes realizar la función de supervisar.

Por otra parte, las directrices EBA se engloban bajo el principio de proporcionalidad. La finalidad del principio es garantizar que todos los sistemas de gobierno, en concreto, los que están relacionados con los procesos de externalización mantengan una coherencia con los riesgos, modelos de negocio, naturaleza y complejidades de las actividades que lleva a cabo la entidad financiera. De esta manera, las entidades son capaces de cumplir con todos los objetivos establecidos por la autoridad supervisora bancaria en el ámbito de la UE.

1.2. Premisas en la externalización de actividades

Las entidades financieras que realizan los procesos de externalización de sus actividades deberán de cumplir con las siguientes condiciones:

- El órgano de administración sigue siendo el responsable de los procesos en relación con los acuerdos que se deben de firmar con los terceros y con la supervisión de que los requisitos establecidos se cumplen adecuadamente.
- Si las entidades deciden externalizar tareas operativas del control interno, deberán de asegurarse de que dichas tareas se están realizando de manera eficiente e incluso pidiendo informes a los proveedores de servicio sobre la ejecución de dichas tareas.

[25] Directrices EBA, *Op. Cit*., artículo 12.

Por otra parte, conforme al artículo 26 de las directrices, las entidades financieras deben de determinar si un acuerdo con un tercero se puede considerar como un proceso de externalización.

En el marco de esta evaluación, se debe de tener en cuenta dos aspectos: (i) si la función (o una parte de la misma) que se externaliza a un proveedor de servicios es desempeñada de forma recurrente o continua por el proveedor de servicios y (ii) si esta función (o parte de la misma) entra en el ámbito de las funciones que desempeñaría o podría desempeñar la entidad o, incluso si la entidad no ha desempeñado por sí misma esta función en el pasado. [26]

En la misma línea, cuando un acuerdo que se vaya a firmar englobe diferentes actividades o funciones, las entidades financieras deberán de evaluar todos y cada uno de los aspectos descritos en el contrato.

Como he mencionado anteriormente, se hace hincapié en la externalización de procesos de carácter esenciales. A continuación, se establecen tres situaciones en las que la entidad deberá considerar la función como esencial y, por consiguiente, tener un control exhaustivo y asegurar el cumplimiento de los requisitos exigidos. Serían las siguientes:

- Cuando un fallo en la función perjudicase notablemente en la continuidad de otras actividades bancarias o en resultados financieros.
- Cuando las tareas que se externalizan son de control interno salvo que se demostrase que un fallo en la ejecución no afectaría gravemente en el control interno.
- Cuando se requiera la autorización de una autoridad competente para externalizar una función.

1.3. Protección de los datos

Estas directrices de la EBA establecen una regulación genérica sobre la protección de los datos. El desarrollo normativo no es muy específico respecto a este riesgo.

A continuación, se exponen los diferentes puntos de las directrices que hacen referencia a la protección de los datos cuando las entidades financieras externalizan alguna de sus funciones o actividades.

[26] Directrices EBA, *Op. Cit*., artículo 26.

Dentro del Título III sobre el marco de gobernanza, se establecen diferentes puntos relativos a los pasos que se deben seguir cuando la entidad financiera decide externalizar una función a través de un proveedor de servicios.

En concreto, el desarrollo normativo en materia de protección de datos está regulado en el apartado 13 el cual trata sobre la fase contractual. Es decir, conforme a las directrices EBA todo lo relacionado con la protección de datos se debe de aclarar y establecer en el momento de la elaboración del contrato y la perfección de éste.

En primer lugar, se establece que en el contrato se deben de dejar por escrito todos los derechos y obligaciones tanto de la entidad financiera como del proveedor de servicios.

En segundo lugar, las entidades financieras deben de confirmar que los proveedores con los que han firmado cumplen con unos sistemas de seguridad correctos y unos controles de seguridad informáticos. Por ejemplo, que estén preparados en el caso de ciberataques.

Por otra parte, cuando las entidades contratan externalizaciones TIC, éstas deben de desarrollar, por un lado, los requisitos que deben de cumplir los proveedores del servicio sobre la seguridad de los datos que se transfieren y, por otro lado, realizar un control continuo para ir comprobando que se están cumpliendo con los requisitos exigidos. Además, se remarca que, en el contexto de "tratamiento o transferencia de datos"[27], se debe de realizar un análisis exhaustivo respecto a los lugares donde se realice la transferencia de datos o el tratamiento y así poder analizar los posibles riesgos de esa zona.

Por último, cuando la externalización de las funciones implica la participación de terceros países se requiere que se cumpla con el desarrollo normativo nacional vigente. Por ello, el artículo 84 establece que las entidades "deberían asegurarse de que el acuerdo de externalización incluya la obligación de que el proveedor de servicios proteja la información confidencial, personal o cualquier otro tipo de información delicada y cumpla todos los requisitos legales en relación con la protección de datos aplicables a la entidad".[28]

[27] Directrices EBA. *Op. Cit.,* artículo 83.
[28] Directrices EBA. *Op. Cit.,* artículo 84.

2. *OFFICE OF THE COMPTROLLER OF THE CURRENCY*

En Estados Unidos, la Oficina del Controlador de la Moneda (OCC) establece una serie de medidas para los bancos nacionales enfocadas a los procesos de externalización de actividades financieras. Estas medidas están recogidas en el boletín 2013-29, de 30 de octubre de 2013. (Office of the Comptroller of the Currency, 2013)

2.1. Objeto de las directrices OCC

La normativa de la OCC va dirigida a todos los bancos nacionales para ayudar y regular todos los riesgos que puede conllevar la externalización de actividades a través de proveedores de servicios. En concreto, se centra en especial cuando se externalizan actividades críticas que son definidas por la OCC como aquellas funciones, actividades o servicios bancarios significativos que pueden tener un importante impacto en las operaciones bancarias.

En suma, la OCC espera que los bancos realicen sus actividades de manera efectiva y que además puedan gestionar los riesgos potenciales independientemente de que la actividad haya sido realizada por el propio banco o por un proveedor de servicios.

Por otro parte, la OCC también explica el término "terceros" estableciendo que es cualquier negocio entre un banco y otra entidad por medio de un contrato o cualquier otro método. Este concepto es definido por la OCC de una manera amplia dando a entender que cualquier actividad puede ser externalizada.

2.2. Premisas en la externalización de actividades

El boletín de la OCC establece tres aspectos relevantes a tener en consideración en la externalización de actividades:

- En primer lugar, se establece que los procesos que desarrollan los bancos para gestionar los riesgos deben ser coherentes con el riesgo y con la complejidad de la relación con el tercero.
- En segundo lugar, los bancos deben de asegurarse de que existe, por un lado, una comprensión adecuada de los riesgos que pueden llegarse a generar y, por otro lado, una supervisión continua del *outsourcing* cuando se trata de actividades críticas.
- En tercer lugar, son efectivos aquellos procesos de gestión de riesgos que incluyen, en todo el ciclo de la relación con los proveedores de servicio, una debida diligencia en la selección del proveedor de servicio, contratos escritos en

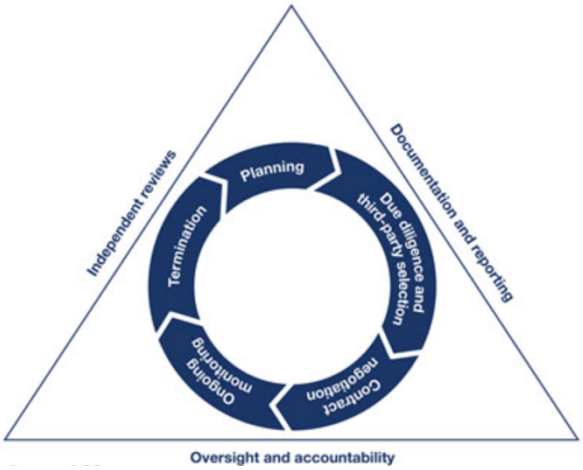
los que se establecen los derechos y obligaciones de las partes y una adecuada vigilancia de las actividades de los proveedores de servicios, entre otros.

En concordancia con el primer punto establecido, la OCC espera que las entidades financieras dispongan de procesos de gestión acordes con el nivel de riesgo, con la complejidad de la relación con los proveedores de servicio y con la estructura organizativa del banco. Por ello, se establece que el proceso de gestión de riesgos será efectivo cuando contenga un "ciclo de vida continuo" el cual deberá incorporar las siguientes fases:

- Planificación: El desarrollo de un plan es a menudo el primer punto en el proceso. La planificación sirve de ayuda en muchas situaciones, pero es esencial que esté presente cuando la relación con proveedores de servicios se basa en actividades críticas. Además, dentro de la fase de planificación entra la selección de los proveedores de servicios con la debida diligencia.
- Negociación del contrato: En la elaboración del contrato, las entidades financieras deben asegurarse de que se definen de manera clara todas las obligaciones y responsabilidades y así asegurar el cumplimiento del contrato y mitigar las disputas que puedan surgir sobre el cumplimiento. Por otro parte, una vez celebrado el contrato es importante realizar un seguimiento continuo de la externalización.
- Terminación: Se debe desarrollar un plan de contingencia para el momento en el que (i) el contrato finaliza, (ii) se cumplen todos los términos, (iii) por incumplimiento del contrato o (iv) como respuesta a cambios de estrategia de la entidad financiera. Como consecuencia, se podrán transferir las actividades a otro banco o que las realice el propio banco, es decir, en este caso se estará produciendo un *insourcing.*

Durante estas fases, las entidades financieras deberán realizar las actividades de control y responsabilidad, de revisiones independientes y de documentación de la información y *reporting.*

FIGURA 2: Risk Management Life Cycle



FUENTE: OCC

2.3. Protección de los datos

En este epígrafe, además del boletín 2013-29, se va a hacer referencia al *frequently asked questions* (FAQ) que se desarrolló como un suplemento del boletín 2013-29.

En consonancia con el boletín 2013-29, la OCC establece en el FAQ el procedimiento que se debe de llevar a cabo cuando la externalización de una actividad se contrata con un proveedor de sistemas tecnológicos. En este caso, hay que tener en consideración dos aspectos que son: (i) la gestión del riesgo es igual de esencial que cuando se contrata con cualquier otro proveedor, y (ii) el nivel de supervisión y de debida diligencia debe ser coherente y proporcional al riesgo asociado con el uso de datos transferidos.

Por ello, cuando se realiza una contratación con un proveedor de sistemas tecnológicos, la entidad financiera deberá de asegurarse que en el contrato se especifica todo lo relacionado con la externalización del servicio. Además, debe de comprender y determinar los controles que debe de realizar el proveedor de servicios y cuáles debe realizar la entidad financiera. Independientemente de esta división, la entidad financiera siempre va a ser la responsable en última instancia.

Por otra parte, la OCC desarrolla en el boletín 2013-29 que en los contratos se debe de establecer que en el caso de que se termine el contrato, los datos del banco se deberán de devolver o eliminar. Además, se debe de realizar un seguimiento continuo del proveedor de servicios hasta que se vean satisfechos los términos del contrato.

En suma, la OCC establece un apartado para desarrollar la normativa relacionada con las responsabilidades que tienen las entidades financieras cuando proveen, reciben o mantienen información. Respecto a los datos, se especifica que el contrato debe de recoger con claridad los procedimientos a seguir y la necesidad de notificación cuando el proveedor de servicios tiene una pérdida de datos.

3. *PRUDENTIAL REGULATION AUTHORITY*

En Reino Unido, la autoridad encargada de establecer la normativa para las entidades financieras en materia de *outsourcing* es la Autoridad Prudencial Regulatoria (PRA). Esta autoridad ha publicado diferentes normativas sobre la regulación de la externalización de actividades. En concreto, a lo largo de este epígrafe se va a desarrollar la normativa sobre *"outsourcing and third party risk management".* (Bank of England, 2021)

Esta normativa es una Declaración de Supervisión (en inglés, *Supervisory Statement*) en la cual la PRA expresa las expectativas que tiene sobre las entidades financieras que están bajo su supervisión a la hora de cumplir con la regulación sobre la externalización y con la gestión de los riesgos de terceros.

3.1. Objeto del SS2/21

En primer lugar, los objetivos del *Supervisory Statement* [29] son tres: (i) complementar los requisitos y las expectativas de la resiliencia operacional, (ii) proporcionar una mayor resiliencia a las entidades financieras y facilitar la adopción de nuevas tecnologías, e (iii) implementar las directrices de la EBA en materia de *outsourcing.*

El *Supervisory Statement* de la PRA define el término *outsourcing* como un negocio formalizado de cualquier manera entre una entidad financiera y un proveedor de servicios y a través del cual éste realiza un proceso, un servicio o una actividad. Además, en línea con las directrices de la EBA, para saber si un contrato con un proveedor de servicios cabe dentro de la definición de *outsourcing* habrá que considerar si el servicio realizado por el proveedor se realiza de forma fija o recurrente. [30]

Cuando un acuerdo de externalización no se puede introducir bajo el concepto de *outsourcing,* la PRA espera que las entidades financieras evalúen los riesgos y la materialidad de las actividades para que no perturben sus objetivos establecidos. Algunos ejemplos de actividades externalizadas que no se pueden definir como *outsourcing* son

[29] Supervisory Statement: *Outsourcing and Third-Party Risk Management*. (SS2/21)
[30] Supervisory Statement. *Op. Cit.,* artículo 2.1.

las compras de hardware o software o la compra de datos recogidos por terceros proveedores.

Por otra parte, esta normativa recoge el principio de proporcionalidad en su artículo número 3.[31] Dicho principio debe ser tenido en cuenta por todas las entidades financieras que aplican esta normativa y consiste en que éstas deberán de cumplir con las expectativas de manera proporcional a su tamaño, su estructura interna, naturaleza o complejidad de sus actividades.

3.2. Premisas en la externalización de actividades

La PRA establece lo esencial que es que las entidades financieras tengan toda la información necesaria y de manera clara sobre los proveedores de servicios con los que se va a externalizar alguna actividad propia del banco. Además, especifica que se deberá de recoger en el contrato todas las características propias de la externalización.

Por otra parte, el *Supervisory Statement* establece una fase llamada "pre-*outsourcing*" en la que se establece lo que la PRA espera de las entidades financieras antes de realizar cualquier tipo de acuerdo de externalización.

Las entidades financieras en la fase pre-outsourcing deben determinar la materialidad[32] de la operación en cada *outsourcing*, actuar con la debida diligencia ante todos los proveedores de servicios potenciales y analizar todos los riesgos que se pueden llegar a generar.

El término materialidad es definido por la normativa como "servicios de tal importancia que la debilidad o el fracaso de los mismos arrojaría serias dudas sobre el cumplimiento continuado por parte de la empresa de las condiciones de umbral o de las Normas Fundamentales". [33]

En la misma línea, para evaluar la materialidad de las actividades cada entidad financiera deberá desarrollar sus propios procesos como parte del proceso principal de evaluar el *outsourcing* y a los proveedores de servicios. No obstante, no existe libertad absoluta, sino que se recogen unos criterios que deben ser cumplidos por las entidades financieras para asegurarse de que los procesos son consistentes. Estos criterios son:

[31] Supervisory Statement. *Op. Cit.,* artículo 3.
[32] El término materialidad es equitativo al término "esencial" usado por la directrices EBA o al término "crítico" usado por las directrices OCC.
[33] Supervisory Statement. *Op. Cit.,* artículo 5.2.

- Se evaluará una actividad como material cuando un fallo o un defecto de ésta pueda afectar a la estabilidad financiera de Reino Unido.
- En el caso de las entidades financieras, deberán de conseguir llegar al umbral de condiciones, cumplir con las Normas Fundamentales, cumplir con la legislación y con el Reglamento PRA y contar con resiliencia operativa.

Cuando la PRA establece que las entidades financieras deben de cumplir con el umbral de condiciones, significa que se debe de cumplir con tres condiciones: (i) que la entidad financiera pueda ser supervisada de manera efectiva por la PRA, (ii) contar con un marco y una estructura organizacional clara y transparente y (iii) llevar el negocio de una manera prudente lo que implica contar con los recursos apropiados tanto financieros como no financieros. [34]

Por último, como se ha mencionado, las entidades financieras deben de cumplir las Normas Fundamentales que establece la PRA para promocionar la seguridad y la solidez de las empresas reguladas. A continuación, se exponen las ocho Reglas Fundamentales:

- Las firmas deben de desempeñar su negocio con integridad.
- Las firmas deben de desempeñar su negocio con la debida diligencia y cuidado.
- Las firmas deben de actuar de una manera prudente.
- Las firmas deben de contar con unos recursos financieras adecuados.
- Las firmas deben de desarrollar unas estrategias y sistemas para gestionar los riesgos.
- Las firmas tienen que gestionar sus asuntos de la manera más efectiva y responsable.
- Las firmas deben de cooperar con sus autoridades reguladoras de una manera apropiada.
- Las firmas deben de estar preparadas para disolverse de una manera ordenada para producir la mínima disrupción.

3.3. Protección de los datos

La Autoridad Prudencial Regulatoria desarrolla este apartado con las expectativas de que la transferencia de datos con proveedores de servicios esté protegida y regulada y,

[34] Supervisory Statement. *Op. Cit.,* artículo 4.6.

además, que dicha regulación esté en consonancia con lo establecido por la EBA en sus directrices.

En primer lugar, el término dato debe ser entendido como "aquellos datos confidenciales, sensibles para la empresa y transaccionales". [35]

Conforme al artículo 7 del *Supervisory Statement,* cuando la externalización de una actividad a través de un proveedor de servicios incluya la transferencia de datos a éste, las entidades financieras deben de definir, documentar y entender las responsabilidades que tendrá el proveedor de servicios y, además, llevar a cabo las medidas necesarias para proteger los datos.

En la misma línea, las entidades financieras deberán clasificar los datos según el grado de confidencialidad y de sensibilidad, identificar los riesgos potenciales que pueden generarse por la transferencia de los datos, acordar con el proveedor un nivel adecuado de confidencialidad y disponibilidad y, por último, obtener toda la documentación posible y necesaria sobre el proveedor de servicios.

Otro aspecto relevante en materia de protección de datos es la exigencia de clasificación de los datos. Las entidades financieras son responsables de que los datos con los que cuenta estén clasificados en categorías como pueden ser confidenciales, sensibles, personales y que todos ellos estén protegidos debidamente. [36]

Por otra parte, la PRA establece que cuando las entidades financieras usan la tecnología de nube para la distribución de sus datos, se producen unos beneficios en la resiliencia operativa, es decir, las entidades financieras pueden tener mayor capacidad para responder y recuperarse ante cualquier adversidad. Además, se espera que las entidades financieras adopten un enfoque basado en el riesgo de los datos de localización y de esta manera puedan, por un lado, aprovechar de los beneficios de la resiliencia operativa, y, por otro lado, puedan gestionar los riesgos potenciales.[37]

En consonancia a lo anterior, las empresas deberán de analizar si sus datos van a ser transferidos y procesados a zonas donde no puedan tolerar el riesgo y en ese caso,

[35] Supervisory Statement. *Op. Cit.,* artículo 7.1.
[36] Supervisory Statement. *Op. Cit.,* artículo 7.5.
[37] Supervisory Statement. *Op. Cit.,* artículo 7.8.

introducir las medidas necesarias para proteger los datos y conseguir mitigar los posibles riesgos.[38]

Respecto a la protección de los datos, la PRA establece que las entidades financieras deben de implementar medidas de protección sobre los datos que transfieren y que estas medidas sean establecidas en sus políticas de externalización.

Además, añade que cuando los datos están encriptados, las entidades financieras deben asegurarse de que las claves de encriptación están protegidas debidamente por ellos y por los terceros.

Por último, la PRA también aclara que los proveedores de servicios deben de contar con un entorno de seguridad para permitir a las entidades financieras funcionar adecuadamente y cumplir con sus responsabilidades.

4. TABLA COMPARATIVA

En este apartado, se realiza una comparativa de la regulación del *outsourcing* en materia de protección de datos personales en las tres zonas analizadas.

En concreto, se realiza la comparativa de diferentes aspectos:

- Las diferentes formas en las que las autoridades establecen sus normas.
- El nivel de definición de términos por parte de la respectiva Autoridad Reguladora y Supervisora. Por ejemplo, si se define el término *outsourcing,* proveedor de servicio…
- Regulación de las actividades o funciones más relevantes y que, por consiguiente, deben ser reguladas y protegidas con mayor detalle.
- Terminología usada por cada autoridad para hacer referencia a las funciones o actividades que son más relevantes.
- Detalles sobre cómo las entidades financieras deben llevar a cabo los procesos de externalización.
- El nivel de detalle con el que la autoridad reguladora y supervisora regula cómo debe realizarse la transferencia de datos a terceros y como se deben de gestionar los riesgos que se generan por contratar con proveedores de servicios.

Por ello, para realizar la tabla comparativa se usan los términos “ALTA”, “MEDIA” y “BAJA” para hacer referencia al nivel de detalle con el que cada Autoridad Reguladora

[38] Supervisory Statement. *Op. Cit.,* artículo 7.9.

y Supervisora de cada zona entra a regular los diferentes aspectos que conlleva un proceso de externalización de actividades o funciones de las entidades financieras. Y, en concreto, cómo está regulada la protección de los datos en cada zona cuando son transferidos a terceros por la externalización de actividades.

TABLA 2: Comparativa de la regulación de la protección de los datos en outsourcing

	EUROPA	**ESTADOS UNIDOS**	**REINO UNIDO**
Normativa	Directrices EBA	Boletín 2013-29	*Supervisory Statement* (SS2/21)
Definición de conceptos	**ALTA**	**BAJA**	**ALTA**
Nivel de concreción de las actividades relevantes	**ALTA**	**ALTA**	**ALTA**
Terminología de las actividades	Esencial o importante	Crítico	Materialidad
Detalles sobre el proceso de externalización	**MEDIA**	**ALTA**	**ALTA**
Regulación de la protección de datos	**MEDIA**	**MEDIA**	**ALTA**

FUENTE: Elaboración propia

CAPÍTULO V. CONCLUSIONES

A continuación, se exponen las distintas conclusiones extraídas a lo largo del presente trabajo.

En primer lugar, las conclusiones generales sobre los riesgos no financieros son:

i. Los riesgos no financieros cada vez están más presentes en el sector financiero y están muy ligados con la externalización de procesos u *outsourcing*.

ii. Será la propia entidad financiera la responsable de cualquier riesgo no financiero potencial que se pueda llegar a asumir como consecuencia de un proceso de externalización.
iii. Las entidades financieras deben ser lo más resilientes posibles para ser capaces de continuar con su funcionamiento ante potenciales disrupciones operacionales.

En segundo lugar, tras realizar el análisis comparativo de la normativa del *outsourcing* en Europa, Estados Unidos y Reino Unido se concluye lo siguiente:

i. Cada autoridad regulatoria y supervisora desarrolló estas directrices sobre externalización en distintos años, lo que puede afectar al contenido normativo.
ii. La OCC es la autoridad que establece unos conceptos menos firmes sobre la externalización de actividades, es decir, es menos específica. Sin embargo, las directrices proporcionadas por las autoridades de Reino Unido y Europa son más rigurosas y extensas.
iii. Respecto a las actividades fundamentales, las tres autoridades establecen en sus directrices cuales son las actividades más significativas y, por consiguiente, cuales deben ser reguladas y supervisadas por las entidades financieras con mayor atención.
iv. Las tres autoridades establecen una terminología específica para hacer referencia a las actividades o funciones significativas.
v. Respecto al proceso de externalización, la autoridad de Estados Unidos y de Reino Unido establecen una directrices mucho más detalladas y concretas sobre cómo las entidades financieras deben de llevar a cabo el proceso de externalización.
vi. Los procesos de gestión de los riesgos deben ser coherentes con el nivel de complejidad de la actividad externalizada.
vii. Las tres autoridades reguladoras y supervisoras establecen la necesidad de que en los contratos se especifiquen todos los derechos y obligaciones de ambas partes.
viii. Todas las directrices expresan que se debe de realizar un seguimiento continuo de la actividad externalizada.

En tercer lugar, se exponen las conclusiones sobre la regulación de la protección de los datos personales en procesos de *outsourcing*:

i. La autoridad de Reino Unido establece las directrices más exhaustivas y concretas sobre cómo las entidades financieras deben llevar a cabo la protección de los datos

de sus clientes cuando un proceso de externalización conlleva un traspaso de información de los clientes.

ii. Las directrices establecidas por la autoridad de Estados Unidos no expresan de manera clara la regulación y protección de los datos personales, sino que hay que dirigirse a un complemento del boletín en el cual se responde al tema en cuestión.

iii. Las tres directrices no son estrictamente obligatorias, ya que se deben de cumplir para que exista un buen funcionamiento del sistema y de la protección de los datos, pero en ningún momento se expresa la obligatoriedad.

En definitiva, después del análisis realizado se puede concluir con que los riesgos no financieros van ligados al proceso de externalización de actividades u *outsourcing* y lo esencial que es que las entidades financieras sean lo más resilientes posible. Por último, la Autoridad Prudencial Regulatoria es la que establece las directrices más detalladas y completas para las entidades financieras sobre el proceso de externalización y, en concreto, de cómo las entidades financieras deben de actuar y proteger los datos personales de sus clientes cuando se produce un proceso de externalización.

CAPÍTULO VI. POSIBLES AMPLIACIONES DEL PRESENTE TRABAJO

El presente trabajo ha consistido en la realización de un análisis de la regulación de la protección de los datos personales cuando las entidades financieras externalizan funciones o actividades. En concreto, el análisis se ha centrado en la normativa de Europa, Reino Unido y Estados Unidos.

Por ello, considero que sería interesante la realización de un análisis comparativo con algún país asiático ya que la cultura oriental difiere más de la occidental en cuanto a aspectos económicos, políticos, sociales… De esta manera, la regulación de los datos personales puede ser muy diferente a las directrices analizadas en el presente trabajo.

Otra ampliación posible puede ser la realización de un análisis exhaustivo del Reglamento DORA debido a que cada vez el mundo está más digitalizado y automatizado, y gracias a este Reglamento se consigue ayudar a las entidades financieras a mitigar los riesgos que están relacionados con la digitalización y, a la vez, ayudar y conseguir que las entidades financieras sean resilientes.

BIBLIOGRAFÍA

Banco Central Europeo. (2019). *Directrices sobre externalización (EBA/GL/2019/02).* Unión Europea.

Banco Central Europeo. (2023). Funciones del Banco Central Europeo.

Banco Central Europeo. (2023). *Mecanismo Único de Supervisión*. Obtenido de Bnaking Supervision: https://www.bankingsupervision.europa.eu/about/thessm/html/index.es.html

Banco de Inglaterra. (2019). *Building Operational Resilience: Impact tolerances for important business.* Obtenido de https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper

Bank of England. (2021). *SS2/21 Outsourcing and third party risk management.*

Bank of England. (2023). *Prudential Regulation*. Obtenido de Bank of England: https://www.bankofengland.co.uk/prudential-regulation

Comisión Europea. (2023). *¿Qué es un responsable o un encargado del tratamiento?* Obtenido de Comisión Europea: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_es

Comisión Federal del Comercio. (1999). *How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act.* Obtenido de Federal Trade Commission: https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act

Comisión Federal del Comercio. (s.f.). *COPPA.* Obtenido de Comisión Federal del Comercio: https://consumidor.ftc.gov/ley-coppa

Consejo de la Unión Europea. (23 de noviembre de 1995). Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. Unión Europea.

Consejo de la Unión Europea. (27 de abril de 2016). Reglamento General de Portección de Datos. Unión Europea.

Consejo de la Unión Europea. (2022). Finanzas digitales: el Consejo adopta el Reglamento sobre la resiliencia operativa digital.

Consejo de la Unión Europea. (27 de Diciembre de 2022). Reglamento sobre la resiliencia operativa digital del sector financiero. Unión Europea.

DPO Centre. (2018). *What is the difference between the DPA 2018 and the GDPR?* Obtenido de DPO CENTRE: https://www.dpocentre.com/difference-dpa-2018-and-gdpr/

European Banking Authority. (2019). Guideling on Outsourcing Arrangements.

European Central Bank. (2023). *Joint Supervisory Teams*. Obtenido de European Central Bank | Banking supervision: https://www.bankingsupervision.europa.eu/banking/approach/jst/html/index.en.html

Financial Stability Institute . (2021). Principles for Operational Resilience.

Galvez, P. (2019). *CBPR y la búsqueda del equilibrio en la protección de datos personales.* Obtenido de Niubox : https://niubox.legal/cbpr-y-la-busqueda-del-equilibrio-en-la-proteccion-internacional-de-datos-personales/

Heywood, J. B. (2002). *El dilema del outsourcing: La búsqueda de la competitividad.* Pearson Education.

Kelly, M. (2020). *¿Qué es la resiliencia operativa?* Galvanize.

López, E. R. (1999). Externalización: Más allá de la subcontratación.

Microsoft . (2023). Ley de privacidad del consumidor de California (CCPA). *Compliance Regulatory*.

Microsoft. (2023). Preguntas más frecuentes sobre la Ley de protección de datos del consumidor de Virginia (VCDPA). *Compliance Regulatory*.

Office of the Comptroller of the Currency. (2013). *Third-Party Relationships: Risk Management Guidance.*

Office of the Comptroller of the currency. (s.f.). *Unites States Government*. Obtenido de https://www.occ.treas.gov/about/who-we-are/index-who-we-are.html

Owen Ryan. (2016). Riesgo Estratégico. La pierda angular para la trasnfromación del riesgo. Deloitte.

PWC. (2018). *Los riesgos no financieros, una amaneza creciente para la banca.* Obtenido de pwc: https://ideas.pwc.es/archivos/20180302/los-riesgos-no-financieros-una-amenaza-creciente-para-la-banca/

Rumold, M. (2016). *necessary&proportionate.* Obtenido de Electronic Frontier Fundation: https://necessaryandproportionate.org/es/country-reports/united-states-america/twenty-sixteen/

Stanjura, Z. (2022). Finanzas digitales: el Consejo adopta el Reglamento sobre la resiliencia operativa digital.

UK Government. (2018). *Data Protection Act*. Obtenido de Legislation.gov.uk: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

UK Government. (s.f.). *Data Protection*. Obtenido de https://www.gov.uk/data-protection

Werther, W. B., & Davis, K. (2008). *Adminsitración de recursos humanos.* MC Graw Hill.