Facultad de Ciencias Económicas y Empresariales
ICADE

RESILIENCIA DIGITAL EN EL SECTOR FINANCIERO: UN ANÁLISIS COMPARATIVO DE DORA Y SU IMPACTO EN EL RIESGO OPERACIONAL A NIVEL INTERNACIONAL

Autor: Andrea María García García
Director: Rafael Castellote Azorín

MADRID | Marzo 2025

RESUMEN

El presente Trabajo Fin de Grado estudia la resiliencia digital del sector financiero a nivel internacional, poniendo como centro de la investigación la Ley de Resiliencia Operativa Digital (DORA). Ante la creciente digitalización de todos los sectores y el cambio hacia una sociedad más tecnológica, DORA aparece como medio de la Unión Europea para erigir la seguridad cibernética en todas las entidades financieras.

El objetivo del estudio es establecer la eficiencia de DORA en la reducción del riesgo operacional y la posibilidad de ser visto como un modelo internacional frente a los marcos reguladores de Estados Unidos y Reino Unido. Para ello, se ha empleado una metodología de investigación cualitativa, buscando las principales diferencias entre los marcos reguladores internacionales.

Los resultados obtenidos indican que DORA es modelo de marco común en la Unión Europea a diferencia de Estados Unidos cuya legislación en esta materia se encuentra mucho más fragmentada, y de Reino Unido cuyo modelo está basado en el principio de "Tolerancia al Impacto". Por ello, DORA sería el candidato ideal de referencia a nivel internacional en términos regulatorios dentro del sector financiero.

Finalmente, las conclusiones dejan ver que, aunque la implementación DORA acarree grandes costes, la necesidad de una regulación que brinde una seguridad digital, es clave para el avance del sector financiero. Además, se plantean mejoras y escenarios hipotéticos que fortalecen al sector en el área de la resiliencia digital.

PALABRAS CLAVE

Resiliencia Digital – DORA – Riesgo Operacional – Ciberseguridad bancaria – Regulación Financiera

ABSTRACT

The study of this Final Degree Project is based on the digital resilience of the financial sector, being focused on the Digital Operational Resilience Act (DORA). Given the growing digitalization of society in all sectors and the change to a more technological society, the European Union issued DORA in order to strengthen cybersecurity in all financial institutions.

The objective of this study is to stablish the efficiency of DORA in the reduction of operational risk and the possibility to be seen as an international model compared to the regulatory framework of the United States (US) and United Kingdom (UK). To do so, the methodology of this investigation has a qualitative approach that looks for the main differences among the international regulatory frameworks.

The results obtained suggest that DORA is a homogeneous model in European Union, contrary to the United States where its legislation is fragmented and the United Kingdom where its model is based in the principle of "Impact Tolerances". Therefore, DORA would be the ideal candidate for the financial sector at an international level regarding digital resilience.

Finally, the conclusions allows to verify that even though DORA's implementation comes with elevated costs (both economic and resources), the need of a regulation that ensures cybersecurity in this sector is key to keep progress on this matter. Furthermore, recommendations are included giving improvement advice and hypothetical scenarios that strengthen the financial sector on this scope.

KEYWORDS

Digital Resilience – DORA – Operational Risk – Banking Cybersecurity – Financial Regulation.

ÍNDICE

INDICE DE FIGURAS

INDICE DE TABLAS

ABREVIATURAS

DORA	*Digital Operational Resilience Act*
TIC	Tecnologías de la Información y la Comunicación
EE.UU	Estados Unidos
FED	*Federal Reserve* (Reserva Federal de EE.UU)
OCC	*Office of the Comptroller of the Currency*
FDIC	*Federal Deposit Insurance Corporation*
BoE	*Bank of England*
FCA	*Financial Conduct Authority*
PRA	*Prudential Regulation Authority*
IBS	*Important Business Services*
EBA	*European Banking Authority*
PS21/3	*Policy Statement 21/3*
SS1/21	*Supervisory Statement 1/21*
UE	Unión Europea

CAPITULO I. INTRODUCCIÓN

1. JUSTIFICACIÓN DEL TRABAJO

En los últimos diez años, el sector financiero ha experimentado una revolución digital sin precedentes que alcanzó un punto de inflexión crítico en el reordenamiento de la industria financiera. En este sentido, la ola de la digitalización financiera es una combinación de tres fenómenos que justifican plenamente la importancia y la necesidad del análisis de este papel, como las blockchain y la inteligencia artificial, la manifestación de riesgos operacionales de naturaleza sistémica, y el surgimiento de marcos regulatorios específicamente diseñados para abordar estos desafíos.

De acuerdo con el Banco de Pagos Internacionales, las instituciones financieras son el objetivo de los ciberataques en 300 veces más frecuencia que en otros sectores económicos. Esto resalta esencialmente la vulnerabilidad del moderno sistema financiero, según BIS Annual Report (2023). Esta información deja ver que la dependencia de las redes tecnológicas en el sector financiero ha establecido un marco en el que incluso los riesgos operacionales pasan a ser de nivel crítico con un efecto cascada que producen graves consecuencias que afectan al sistema financiero local e internacional en su conjunto. Esta vulnerabilidad se ve amplificada en la medida que alcanza a valorarse, debido al incremento de la adopción de tecnologías emergentes como la computación en la nube, la inteligencia artificial o las APIs abierta, según Chen (2020) la finalidad de estas tecnologías es de hacer más operativas, pero a la vez introducen nuevos vectores de riesgo que requerirán un enfoque más meticuloso y global de la gestión de la seguridad. La complejidad de estos riesgos se ve ampliada por la interconexión global de los sistemas financieros, dónde un incidente en una jurisdicción, puede tener repercusiones inmediatas en otras regiones.

Hay que hacer notar que, los incidentes de seguridad más recientes han evidenciado la necesidad de los bancos a robustecer los marcos de resistencia digital. Según el informe presentado por la asociación de parques científicos y tecnológicos de España, APTE (2024), constatan que se han multiplicado las ciber amenazas a las

entidades financieras a raíz de los ataques Ramsomware en los últimos dos años, con previsiones de afectación económica de miles de millones de euros para la Unión Europea. Tales hechos son prueba de las constantes y crecientes severidades en las amenazas y del continuo fracaso de las estrategias tradicionales en torno a la gestión de los riegos operativos. El Operational Resilience Act, desde ahora (DORA), que reclama la Unión Europea como respuesta regulatoria sin igual es necesaria para dar sentido de examen frente a esta reciente situación.

La digitalización también ha reconfigurado los modelos operativos convencionales. La implementación a gran escala de servicios financieros digitales ha incrementado de manera exponencial la superficie de ataques para amenazas cibernéticas. Conforme a la indagación efectuada por CTI-TEND (2024): "Los ataques de phishing siguen centralizados en sectores como el financiero y sanitario por dos motivos, ganancia económica y valor de los datos. En el caso del sector financiero se centran en la suplantación de entidades bancarias o plataformas de pago, buscando obtener datos de usuarios y credenciales".

Tal circunstancia ha dado lugar a lo que correspondería calificar como la paradoja de la modernización financiera, ya que, por un lado, la digitalización da lugar a niveles de eficiencia operativa y disponibilidad de servicios financieros sin actos precedentes, pero, por otro, también el riesgo a errores sucesivos y los riesgos sistémicos se multipliquen exponencialmente. Hechos tan relativamente recientes como el colapso temporal de sistemas de pagos interbancarios en diversos lugares del mundo han puesto de relieve que un determinado acontecimiento que tiene lugar en un punto del tiempo va provocando efectos que se transmiten con rapidez por todo el conjunto del sistema financiero mundial.

Por lo anterior expuesto, la investigación sobre la resiliencia digital en la práctica financiera hace referencia a la progresiva importancia de la tecnología en lo que respecta a la práctica de las transacciones financieras y de la necesidad de poder garantizar la estabilidad y la seguridad del sistema financiero. Además, se realizará un análisis comparativo de DORA y su Impacto en el Riesgo Operacional a Nivel Internacional que ayudará a conocer los diferentes métodos de prevención de aquellos riesgos clasificados como tecnológicos.

2. OBJETIVOS

Este trabajo busca analizar críticamente la eficacia de DORA como marco regulatorio para fortalecer la resiliencia operacional digital en el sector financiero. Para ello, se evaluará su capacidad para mitigar riesgos tecnológicos, como ciberataques, fallos en infraestructuras tecnológicas o brechas en la continuidad del negocio, tomando como referencia casos prácticos en la Unión Europea. Además, se examinarán las implicaciones de su implementación, desde los costes de adaptación para entidades financieras hasta su impacto en la competitividad de mercados emergentes con estándares menos rigurosos.

Por otro lado, el estudio pretende determinar si DORA podría convertirse en un estándar a nivel europeo para la gestión del riesgo tecnológico. Finalmente, se propondrán recomendaciones para superar barreras de armonización internacional, considerando desafíos como la fragmentación regulatoria y la asimetría tecnológica entre regiones, con el fin de construir un ecosistema financiero digitalmente resiliente.

2.1. Objetivo específicos

OE1. Analizar los requisitos de gobernanza digital establecidos por DORA para comprender su estructura y aplicación en la gestión de riesgos tecnológicos en el sector financiero.

OE2. Evaluar los marcos de gestión de riesgos TIC propuestos por DORA para determinar su eficacia en la identificación y mitigación de amenazas tecnológicas.

OE3. Comparar DORA con otros marcos regulatorios internacionales para identificar convergencias y divergencias que puedan influir en la adopción de estándares globales de resiliencia operacional digital.

3. METODOLOGÍA DE LA INVESTIGACIÓN

La metodología que sigue este Trabajo Fin de Grado está enfocada en un método de análisis cualitativo sobre la validez del DORA y comparativo frente a las diferentes regulaciones relacionadas a esta materia en Estados Unidos y Reino Unido. Se recopilará información de fuentes oficiales de diversas autoridades bancarias, así como documentos y artículos que tengan como contenido principal este tema. Posteriormente, se desarrollará una descripción y un examen crítico del escenario actual del sector bancario internacional. De esta manera, se podrán deducir las consecuencias a largo plazo de la implantación de estas normativas.

CAPITULO II. ENTORNO ACTUAL DEL SECTOR BANCARIO

1. RIESGOS NO FINANCIEROS

El contexto actual caracterizado por una profunda transformación digital además del surgimiento de nuevas normativas ha repercutido significativamente en el sector bancario. Esta transformación ha dificultado la situación y exposición de las entidades financieras a estos nuevos riesgos, muy dispares a los ocurridos previamente en este sector en los últimos años.

Los riesgos no financieros tienen una creciente influencia por la estabilidad operacional y resiliencia institucional que generan. Diferentes sucesos como ciberataques, la pandemia o el cambio climático han dado lugar a una necesidad imperante de implantar fuertes estrategias que permitan conseguir una gestión eficiente de este tipo de riesgos.

Según el informe realizado de los riesgos no financieros de KPMG (2022) se pueden diferenciar las siguientes taxonomías o categorías de riesgos en este entorno:

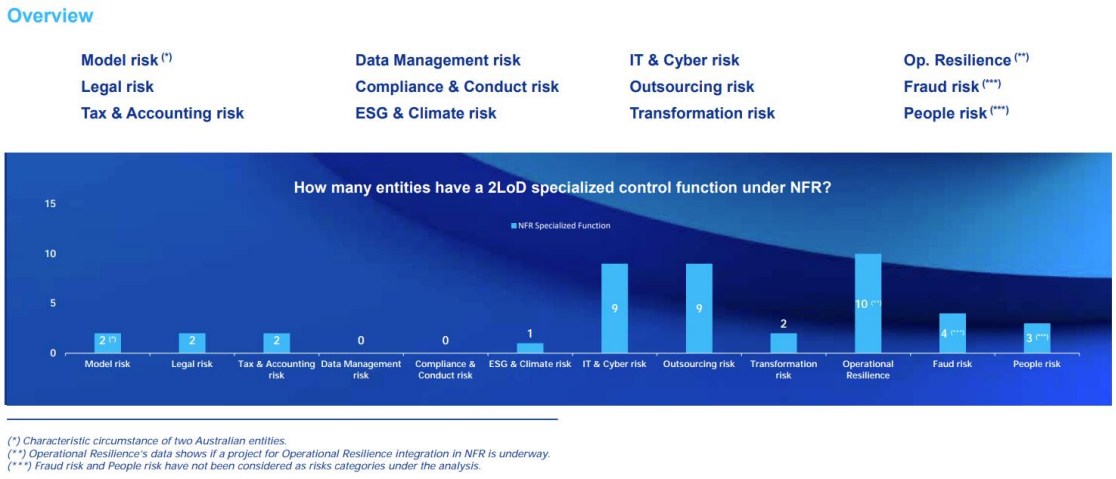


FIGURA 1. Taxonomías de Riesgo

Fuente: KPMG, 2020.

Por un lado, se puede observar que de las 15 entidades que admiten un control 2LoD[1], categorizan como riesgos no financieros con más relevancia a los riesgos tecnológicos y cibernéticos, al riesgo operacional y al riesgo de externalización u outsourcing[2]. Esto indica que la implementación de prácticas que mitiguen estos riesgos está cada vez más demandada por entidades financieras ya que tienen que hacer frente a estas amenazas a las que están expuestas.

Riesgos tecnológicos y cibernético. Este riesgo está definido por el Instituto de Gestión de Riesgos (IRM – Institute of Risk Management) como cualquier pérdida financiera, disrupción o daño causado a la entidad por cualquier tipo de fallo en los sistemas tecnológicos de la misma. Entre los diferentes tipos de ataques cibernéticos que Marsh (2022) identifica en su artículo, se encuentran:

- Vectores de ataque cibernético
- Malware
- Keyloggers
- *Phising*
- Spoofing
- DDoS (Denegación de Servicios)

Como mencionado anteriormente, según CTI-TEND (2024) los ataques más recurrentes en el sector financiero de tipo cibernético son los de *phishing* y en segundo lugar, estarían los DDoS.

Este riesgo está ganando cada vez más relevancia en este sector, según Funcas (2024) el número de ciberataques en el primer semestre de 2024 han aumentado en un 24,7%, un 14% más en el mismo periodo en el año 2023. Se resalta que, a pesar de que las medidas preventivas de seguridad tecnológica implementadas sean efectivas, sigue persistiendo el aumento de estos ataques. Incrementando así, la preocupación del sector financiero en este tipo de riesgo.

[1] **2LoD**: Second Line of Defense o Segunda Línea de Defensa. Este concepto se utiliza para la gestión de riesgos y cumplimiento. Para ello establecen políticas de implementación y se monitorizan esos riesgos.

[2] **Externalización u outsourcing**: contratación de una empresa o profesional independiente para realizar la actividad necesaria por parte de la entidad contratante.

Riesgo Operacional. El Banco de España (2006) define el riesgo operacional como aquel que deriva de un fallo en los procesos internos, de los empleados o de acontecimientos externos. El riesgo operacional ha ido ganando relevancia con los años, especialmente en la actualidad por eventos disruptivos que han hecho temblar la estabilidad y resiliencia del sector financiero. En base al informe Revista RUE (2024) y Banco de España (2006) se pueden identificar diversos factores que aumentan el riesgo:

- Aumento de ciberataques.
- Regulaciones más estrictas para este sector.
- Eventos externos inesperados como el COVID-19 o la guerra de Ucrania.

Se profundizará en el impacto de este riesgo más adelante, debido a la importancia que tiene dentro de las regulaciones relacionadas con el sector bancario.

Riesgo de Externalización (Outsourcing). La externalización de servicios se define como la contratación de servicios externos especializados para dar soporte en el desarrollo de actividades concretas a una entidad contratadora. Esto ha conllevado que se establezcan controles de evaluación de calidad del servicio prestado y la continuidad del negocio.

Según KPMG Tendencias (2018) se estableció de forma predictiva que las crecientes presiones tanto regulatorias como de costes y diferenciación dan lugar al claro incremento de las externalizaciones en este año 2025. Es por ello que hay una necesidad de establecer una estrategia de externalización centralizada, ya que en el caso contrario se podrían obtener las siguientes consecuencias:

- Pérdida de conocimiento para el desarrollo de la actividad.
- Desorden de organización de proveedores de actividades y servicios.

Ante esto, las entidades bancarias deberán tener identificados y controlados sus proveedores tanto internos como externos e implicar a los departamentos de estas externalizaciones para poder cumplir más tarde con las funciones de cumplimiento de estas nuevas regulaciones no financieras.

Estos riesgos, como determinados previamente, son aquellos que están

comenzando a generar preocupación en el sector y por los que las entidades bancarias están motivadas a supervisar y llevar un control más exhaustivo sobre ellos. Sin embargo, en este contexto, se pueden clasificar también como no financieros a:

- Riesgos ESG
- Riesgos reputacionales
- Riesgos legales o de cumplimiento
- Riesgos de transformación

Aunque no generen la misma preocupación que los tres riesgos más destacados, no es sinónimo de que no sean considerados de cara a la implementación de políticas o controles para la mitigación de éstos.

2. IMPACTO DEL RIESGO OPERACIONAL

El riesgo operacional en el ámbito bancario tiene implicaciones de carácter multidimensional lo que comporta unos efectos económicos directos, repercusiones sobre la reputación de las entidades y repercusiones para la continuidad de la actividad de las propias entidades. De acuerdo con el informe realizado por la Autoridad Bancaria Europea (EBA) hace un seguimiento continuo de cuáles son las principales determinaciones que los bancos europeos consideran que explican el riesgo operacional.

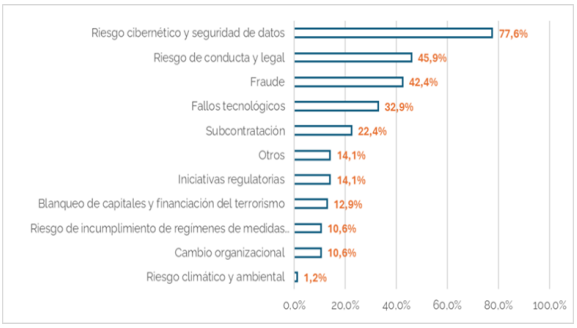


FIGURA 2. Determinantes del Riesgo Operacional

Fuente: EBA Risk Assessment Questionnaire (2024).

La Figura 2 representa el alcance de los bancos europeos encuestados que sostiene que las situaciones señaladas a continuación afectan de forma relevante al riesgo operacional de las entidades en el medio bancario. En el último cuestionario cumplimentado (marzo de 2024), el riesgo cibernético y la seguridad de los datos se presentan, de forma muy relevante, como factores determinantes del riesgo operacional para los propios bancos europeos (77,6%). Un 77,6% en ese sentido, representa que cerca de 8 de cada 10 entidades europeas consideran que el riesgo cibernético constituye una determinación importante en el perfil del riesgo operacional de las entidades. Según la EBA, el avance de la tecnología, la creciente sofisticación, la creciente dependencia con soluciones digitales, pero también las crecientes capacidades de los delincuentes cibernéticos explican por qué los bancos están cada vez más preocupados por este tipo de incidentes. De forma relacionada, un 32,9% de los bancos encuestados también remiten los fallos tecnológicos como un factor importante del riesgo operacional. Además, estos problemas tecnológicos pueden afectar a las capacidades operativas de las entidades financieras en el momento de proporcionar funciones y servicios como operaciones y pagos que se consideran de una importancia crítica ya que podría afectar a la estabilidad financiera.

Del mismo modo, el impacto reputacional asociado con los fallos operacionales es muy significativo. Las interrupciones de los procesos, sobre todo las vinculadas a ciber incidentes, afectan la confianza de los clientes y perjudican la proyección de la institución. La percepción negativa provocada por estas incidencias puede extenderse en el tiempo y afectar la competitividad y la posición óptimas de la organización en el sector.

La continuación del negocio, por su parte, también resulta decisiva. Los acontecimientos operacionales relevantes están provocando daños por interrupciones de servicios críticos, lo que se manifiesta a través de la pérdida de cuota de mercado y el incremento de los costes introducidos por las inversiones necesarias para adaptarse a la normativa. Las inversiones no previstas en infraestructura y los controles no deseados para recuperar la plena operatividad colocan al sector en una situación de presión financiera elevada.

Por lo tanto, se hace necesario integrar medidas de mitigación para los riesgos

operacionales de manera global, es así como el DORA establece un marco normativo orientado a reforzar la resistencia operacional digital, con la implementación de protocolos y controles que, si bien no son una solución por sí mismos, pueden entrar en su lugar, como punto de partida. Sin embargo, debido a su complejidad y rápido desarrollo de los riesgos, especialmente en un entorno digitalizado e interconectado globalmente, será necesario que las instituciones financieras establezcan sus propias estrategias muy robustas y adaptativas que den respuesta a la normativa, ya que sólo así pueden garantizar ser capaces de proteger su estabilidad financiera y su reputación en el largo plazo.

3. CASO REAL: ENTIDAD AFECTADA POR RIESGOS NO FINANCIEROS.

En mayo del pasado año, el Banco Santander fue víctima de un ciberataque a través de un proveedor externo, que acabó filtrando una cantidad masiva de datos, dando a conocer información confidencial tanto de clientes como empleados. Los datos filtrado incluían nombres, direcciones, números de identificación, detalles de cuentas bancarias y números de la seguridad social (Infordisa, 2024). Los países principalmente afectados fueron España, Chile y Uruguay. Según ABC (2024), Banco Santander en el intento de calmar a sus clientes, confirmó que este ataque no afectó a la operativa ni las contraseñas de los mismos.

3.1. Riesgos no financieros identificados en el caso

En base a la explicación previa de cada uno de los riesgos en el apartado 1, se pueden identificar los siguientes riesgos no financieros a los que tuvo que hacer frente Banco Santander cuando sucedió en este caso:

- **Riesgo de Ciberseguridad:** Banco Santander tuvo que hacer frente al ataque cibernético que resultó en un acceso y filtración de datos sensibles de sus clientes y empleados. Esto supuso un incremento de medidas de forma inmediata e inesperada con el fin de fortalecer los sistemas tecnológicos de protección de datos del banco, mitigando así el riesgo de que ocurriese un ataque de mayor envergadura.

- **Riesgo de outsourcing:** el problema del ciberataque residió en la brecha de un proveedor externo. La contratación de servicios externos o de terceros puso al Banco Santander en una situación vulnerable y más expuesto a la posibilidad de un ciberataque mayor.
- **Riesgo de cumplimiento:** En este caso, la filtración de datos de empleados y clientes supone el incumplimiento del Reglamento General de Protección de Datos (RGPD) ya que los datos filtrados eran, precisamente, datos personales de estas personas.
- **Riesgo operacional:** como explicado en el riesgo de ciberseguridad, el ataque sucedió de forma inesperada y Banco Santander tuvo que tomar medidas de contingencia de fortalecimiento de sistemas de seguridad tecnológica de forma inmediata para poder hacer frente a este ataque.
- **Riesgo reputacional:** ante esto, Banco Santander se vio afectado en la pérdida de confianza de los clientes. Esto normalmente tiene un impacto negativo en términos económicos y una imagen negativa de la entidad.

3.2. Relevancia de DORA en este caso.

La creciente dependencia de la tecnología en el sector financiero ha dado lugar a una serie de vulnerabilidades no financieras que amenazan la operatividad y estabilidad de las instituciones. Los ataques cibernéticos según Cremer, et al. (2023), han evolucionado en sofisticación, existiendo grupos criminales que orientan sus esfuerzos a infraestructuras críticas, con lo que puede resultar en la paralización de operaciones críticas junto con la exposición de datos sensibles y la exigencia de pagos elevados para restablecer el funcionamiento habitual. En este contexto, la legislación DORA establece medidas para la mejora de la resiliencia operativa digital, facilitando la implementación de controles y protocolos de seguridad que, en parte, abordan algunos de estos riesgos.

La integración de entidades proveedoras de servicios en la nube junto con otros terceros en la operativa bancaria ha aumentado la superficie de ataque, por lo que la

cadena de suministro tecnológico se convierte en el tráfico de entrada crítico para el vector que contiene las vulnerabilidades. Los ciber delincuentes pueden beneficiarse de las vulnerabilidades derivadas de las actualizaciones de software o de los mecanismos de control y de transparencias de estos proveedores para acceder de forma indebida a sistemas sensibles. El DORA reconoce la importancia de gestionar los riesgos derivados de terceros y establece requisitos para la supervisión y control de los proveedores críticos, permitiendo de esta forma mitigar indirectamente los agujeros de seguridad derivados de esta vulnerabilidad.

En este caso, confirmamos la necesidad de la implantación de DORA ya que el Banco Santander hubiese podido evitar afrontar estos riesgos o haberlos mitigado en el momento del ataque de forma más efectiva. En especial, el riesgo de terceros que es por el que fue causado este ataque.

CAPITULO III. DORA: DIGITAL OPERATIONAL RESILIENCE ACT

1. NECESIDAD DE DORA EN ESTE SECTOR

La evolución del sector financiero hacia un marco cada vez más digital ha puesto de manifiesto la necesidad de un marco regulador unificado para la gestión de los riesgos tecnológicos y operacionales. Antes de la llegada de DORA, el marco regulatorio europeo era uno de alta fragmentación, en el que todos los Estados miembros les asignaban un sentido único a las exigencias de resistencia digital. Esto último generaba ineficiencias para todas las entidades del sector financiero que operan en varios marcos normativos, teniendo que lidiar con un complejo mosaico de requisitos regulatorios nacionales.

Los últimos datos recabados por el Banco Central Europeo subrayan la urgente necesidad de esta regulación. En lo que respecta a las brechas relacionadas con las TIC, entre los años 2016 y 2021 se ha producido un creciente incremento del 54% en cuanto a los incidentes tecnológicos de gran consideración civil, con unos costes que superan los 85.000 millones de euros. Este incremento es la impronta del aumento de la complejidad de las amenazas TIC y de una creciente interdependencia entre las entidades de supervisión de las TIC, cada una de las cuales ha contribuido al nacimiento de nuevos vectores de riesgo sistémico.

La digitalización del sector ha permitido la aparición de nuevos modelos de negocio, principalmente relacionados con la tecnología financiera. En este proceso, la dependencia de proveedores de servicios y de tecnología elevada ha aumentado, materializándose el entrelazamiento de las interdependencias tecnológicas que afectan a la eficacia del proceso de supervisión, el cual se ha de llevar a cabo de forma coordinada y eficaz. Por fin, la falta de estándares generales y de prácticas comunes en la gestión del riesgo TIC y en la evaluación de la resiliencia operacional ha ido provocando cada vez más inquietud en la comunidad de supervisores y reguladores.

2. ÁMBITOS DE APLICACIÓN Y REQUISITOS

2.1. Ámbito de aplicación

Según DORA, el ámbito de aplicación está claramente definido en el Artículo 2 del Reglamento. El presente se aplicará a las denominadas entidades financieras que incluyen las "entidades de crédito, entidades de pago, proveedores de servicios de información sobre cuentas, entidades de dinero electrónico, empresas de servicio de inversión, proveedores de criptoactivos, depositarios centrales de valores, entidades de contrapartida central, centros de negociación, registro de operaciones, gestores de fondos de inversión alternativos, sociedades de gestión, proveedores de servicios de suministro de datos, empresas de seguros y reaseguros, intermediarios de seguros, fondos de pensiones de empleo, agencias de calificación crediticia, administradores de índices de referencia cruciales, proveedores de servicio de financiación participativa, registros de titulizaciones y proveedores terceros de servicios de TIC."

Además, es importante resaltar que el Reglamento señala en el Artículo 1 que éste es aplicable a todas aquellas entidades financieras mencionadas en el Artículo 2 que estén dentro de la Unión Europea.

En este aspecto, debemos tener en cuenta el principio de proporcionalidad mencionado en el Artículo 4: "Las entidades financieras aplicarán las normas establecidas en el capítulo II de conformidad con el principio de proporcionalidad, teniendo en cuenta su tamaño y perfil de riesgo general, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones."

2.2. Requisitos

DORA crea un marco regulatorio exhaustivo que contempla los retos de la resiliencia operacional digital mediante cinco áreas principales interrelacionadas. En primer lugar, la regulación requiere que se determinen marcos robustos de gestión de los riesgos tecnológicos los cuales tienen que encajarse plenamente dentro de los

sistemas generales de gestión de los riesgos de las entidades financieras. Ello implica no sólo la puesta en marcha de controles técnicos sino también la creación de una cultura organizativa para que la resiliencia digital tenga un enfoque prioritario en todos los niveles de la organización.

Según INCIBE (2024), los requisitos DORA se estructuran en cuatro pasos en los que se incluyen: la gestión y gobernanza del riesgo de TIC, notificación de incidentes, pruebas de resiliencia e intercambio de amenazas y gestión de riesgos de terceros.

Cada uno de estos requisitos se encuentran en diferentes artículos del Reglamento. Éstos están distribuidos de la siguiente forma:

Gestión y gobernanza del riesgo de TIC – Capítulo II.

Este capítulo recoge los artículos 5 al 16 en los que se centra en la gestión y gobernanza del riesgo TIC. Este capítulo está dividido en dos secciones:

En la Sección I se encuentra el artículo 5 del Reglamento que establece que todas las entidades financieras a las que les aplica esta normativa deberán definir una estructura interna o de gobernanza que asegure la gestión del riesgo de las TIC. Esto se refiere a un responsable o responsables que lleven a cabo la implantación o aplicación de DORA en su entidad asumiendo la responsabilidad de este tipo de gestión, adoptando políticas que la respalden y mantengan una monitorización de las prácticas implementadas relacionadas a la misma. En este artículo, también, se especifica qué canales de comunicación deberá establecer este responsable para estar perfectamente informado respecto aquellos acuerdos firmados con proveedores externos de servicios TIC, potenciales variaciones en la relación con los proveedores terceros de servicios TIC y las consecuencias de dichos cambios para así poder analizar el impacto de las actuaciones que deberán ser puestas en marcha y monitorizadas posteriormente.

En la Sección II se encuentran el resto de los artículos, que establecen el marco sobre el que se gestionará el riesgo relacionado con las TIC por el que se les obliga a las entidades financieras a desarrollar estrategias, políticas, procedimientos y

protocolos y herramientas de las TIC además de especificar cada uno de los criterios que deben tener cada una de ellas.

Gestión, clasificación y notificación de incidentes relacionados con las TIC – Capitulo III

Del artículo 17 al 23 se recogen los requisitos que la Regulación demanda para la segunda fase de implantación en las entidades financieras. Esta fase esta basada en la Identificación de Incidentes, es decir, consiste en identificar, reconocer y notificar el número de ocasiones en los que se produce un incidente de seguridad dentro de la entidad financiera.

En el artículo 17 del Reglamento, vuelve a establecer la importancia de un marco interno de gobernanza eficiente mediante la definición de políticas y procedimientos que consigan identificar y mitigar los incidentes ocasionados por las TIC. Esto permite seguir un proceso ordenado y eficiente para la gestión de los riesgos. Este proceso deberá estar establecido previamente de forma clara y ordenada por un equipo especializado y formado en esta materia, garantizando una rápida respuesta frente a cualquier tipo de incidente ocasionado en la entidad.

En el artículo 18 del Reglamento, se especifica la importancia de la clasificación de los incidentes en función del impacto ocasionado en la continuidad del servicio de la entidad financiera (una incidencia que interrumpa por completo un servicio financiero crítico se podría considerar una incidencia de carácter grave). Además de la clasificación, se garantiza una asignación de recursos de forma más eficiente y se da preferencia a aquellos incidentes que puedan generar consecuencias directas en la estabilidad de la entidad financiera mediante una evaluación de éstos que especifican la urgencia con la que deben ser tratados.

En el resto de artículo incluidos en este capítulo (art.19-23), se presenta la obligación de notificación de incidentes graves a las autoridades correspondientes y en ciertas ocasiones, a las partes afectadas por el mismo. Según el Reglamento, las entidades están obligadas a notificar de forma urgente en el momento de

confirmación de la incidencia y se debe detallar la naturaleza, los sistemas afectados, la duración, la clasificación del impacto, la evolución y las acciones que se han de llevar a cabo para mitigarlo. Asimismo, se incluye un plazo de notificación de 4 horas para poder asegurar que la información fluya adecuadamente conforme a los canales apropiados. Una vez quede notificado, las entidades deberán valorar su respuesta frente al suceso y extraer los fallos cometidos para poder mejorar en caso de un nuevo incidente.

Pruebas de resiliencia operativa digital – Capitulo IV

El capítulo IV del Reglamento recoge los artículos 24 al 27 y la tercera fase que trata sobre la realización de las pruebas de resiliencia operativa digital. De esta forma, las entidades financieras pueden confirmar que sus sistemas e infraestructuras tecnológicas están protegidos frente a los incidentes ocasionados relacionados con las TIC.

El artículo 24 establece los requisitos generales que deben cumplimentar las entidades financieras para poder llevar a cabo las pruebas de resiliencia operativa digital. Así, podrán valorar el curso de preparación y gestión de estos incidentes relacionados con las TIC o identificar las debilidades o carencias relacionadas a esta materia.

El artículo 25 especifica el tipo de pruebas que se realizan a las herramientas y sistemas de TIC de la entidad financiera. Éstas incluyen: “Evaluaciones y exploraciones de vulnerabilidad, análisis del software de código abierto, evaluaciones de seguridad de la red, análisis de carencias, exámenes de la seguridad física, cuestionarios y soluciones de software de detección, revisiones del código fuente cuando sea posible, pruebas basadas en escenarios, pruebas de compatibilidad, pruebas de rendimiento, pruebas de extremo a extremo y pruebas de penetración”.

El artículo 26 introduce las pruebas de penetración basadas en inteligencia de amenazas, estas son más sofisticadas porque simulan ataques cibernéticos avanzados y como principal objetivo evalúan las amenazas reales, detectar las vulnerabilidades y optimizar la capacidad de respuesta ante ciberataques. Se establece que estas pruebas deben ser realizadas cada tres años y deben tener una supervisión directa de

las autoridades competentes.

Por último, en el artículo 27 se especifican los requisitos que se deben aplicar a las pruebas de penetración basadas en amenazas. El principal requisito que se dicta en este artículo es que aquellos encargados de evaluar las pruebas deben ser independientes y contar con la suficiente experiencia, especialmente acreditada por diferentes certificaciones en ciberseguridad y que asegure que la información manipulada durante las pruebas será tratada de forma confidencial.

Gestión del riesgo relacionado con las TIC derivado de terceros – Capitulo V

La última fase de implantación queda recogida en el Reglamento en el Capítulo V en los artículos 28 al 44. En estas secciones el DORA trata de regular y reforzar la seguridad y estabilidad de las entidades financieras por el riesgo que éstas asumen proveniente del *outsourcing* con servicios relacionados a las TIC. Este capítulo está dividido en dos secciones principales:

En la Sección I, el Reglamento trata de definir la gestión del riesgo de terceros (art.28-33) incluyendo los principios generales de este tipo de gestión, lo que deben incluir las cláusulas contractuales y el registro y supervisión de los proveedores de servicios TIC. En los artículos 28 y 29 se incluyen los requerimientos exigidos a las entidades financieras para realizar una buena gestión del riesgo de externalización que precisa del principio de proporcionalidad para poder conseguir una adaptabilidad adecuada al tipo de riesgo al que las entidades están expuestas (naturaleza, escala, complejidad e importancia) y la obligación de la realización de evaluaciones previas a los acuerdos contractuales con los proveedores donde se analice el historial en calidad cibernética y el cumplimiento de las condiciones mínimas para la contratación de esos servicios.

En esta sección se incluye, también, el artículo 30, el cual introduce cómo tienen que ser las cláusulas fundamentales que se deben incluir con los proveedores al formalizar un contrato, asegurando una continuidad del servicio, seguridad de la información y la admisión de derechos de auditoría y supervisión por parte de la entidad contratante.

En la Sección II del Reglamento se define los requisitos de designación y supervisión a los proveedores esenciales de servicios TIC. En los artículos 31 y 32 se establecen los criterios de designación y estructura del marco de supervisión, los cuales todas las entidades financieras están obligadas a cumplir antes de realizar la supervisión de los proveedores. En el resto de los artículos de esta sección se definen las tareas, facultades y ejercicios que los supervisores principales deben tener para que la actividad de supervisión sea lo más efectiva y correcta posible, pudiendo así minimizar los impactos de incidentes que puedan ocurrir en ocasiones futuras.

3. VENTAJAS Y DESVENTAJAS DE LA APLICACIÓN DE DORA EN LAS ENTIDADES FINANCIERAS

DORA, como se ha especificado anteriormente, es un Reglamento que ha sido desarrollado en la Unión Europea para conseguir la armonización en la gestión de la resiliencia operativa digital del sector financiero, especialmente en las entidades bancarias. Esto supone grandes ventajas en materia de protección frente a las amenazas digitales a las que el sector se ve envuelto actualmente. Entretanto, también constituye un factor importante de dificultad para la regulación aplicable a los distintos sectores del ámbito financiero. De su implementación provendrán unos costes bastante altos, que requerirán notables inversiones en términos de tecnología, de formación del personal o de adaptación de los procesos. Las entidades más pequeñas podrían encontrar especialmente costoso el cumplimiento de los requisitos más técnicos de la regulación, como las pruebas avanzadas de resiliencia o la implementación de sofisticados sistemas de monitorización.

Asimismo, no se puede menospreciar la complejidad operativa que se introduce con DORA. Las entidades financieras tendrán que adecuar los procesos actuales, implementar nuevos controles y establecer en las entidades unos principios de buenos hábitos de gobierno y supervisión robustas; un nuevo papel para asegurar la victoria de la implementación de DORA. Los plazos para implementar la regulación regular son ajustados y requerirán la coordinación del esfuerzo entre múltiples entidades participantes, entre distintos departamentos de trabajo o entre distintos proveedores. Este hecho supondrá un reto importante para la gestión del cambio organizativo.

A pesar de estos retos, el balance general sugiere que DORA representa un paso necesario y positivo hacia un sector financiero más resiliente. La regulación da lugar a un marco coherente para gestionar los riesgos emergentes de la digitalización, pero al mismo tiempo podrá vincularse con los requisitos para acometer una innovación más ágil o integradora y una competitividad del sistema financiero europeo. De la eficacia de la implementación de la regulación se dependerá muy en gran medida la capacidad por parte de los reguladores y las entidades financieras para trabajar conjuntamente en la superación inicial de sus desafíos y en el último tramo, con la obtención de los beneficios a largo plazo que puede resultar de un marco armonizado de resiliencia operacional digital.

CAPITULO IV. ANÁLISIS COMPARATIVO INTERNACIONAL

Como se ha estudiado en otros apartados, la Ley de Resiliencia Operativa Digital (DORA) significa un claro progreso en la regulación de ciberseguridad y resiliencia operativa dentro del sector financiero de la Unión Europea. Sin embargo, a nivel global, no es la única propuesta realizada ya que en otros países como Estados Unidos, Inglaterra, LATAM, Canadá, Australia, Singapur…han impulsado el fortalecimiento de estos riesgos con marcos regulatorios enfocados en los mismos objetivos que DORA. Este análisis comparativo estará centrado en las iniciativas de Estados Unidos y de Reino Unido.

1. RESILIENCIA OPERATIVA DIGITAL EN ESTADOS UNIDOS

En Estados Unidos, la Reserva Federal (FED) ha trasladado su preocupación por los riesgos cibernéticos en el sector financiero estadounidense. Según Bamber y Fernández-Stark (2022) los ciberataques se han multiplicado en América del Norte, llegando a aumentar su cifra de inversión en US$30.7 billones en cinco años para protegerse de ataques cibernéticos en ambos sectores público y privado. Ante esto y en respuesta a la preparación del sector financiero frente a estos ataques, la FED y otras agencias reguladoras estadounidenses como la OCC (Office of the Comptroller of the Currency) y la FDIC (Federal Deposit Insurance Corporation) han desarrollado cuadros supervisores dónde establecen estrictas directrices en relación con los riesgos tecnológicos y reporte de incidentes. Según la Junta de Gobernadores del Sistema de la Reserva Federal (2024), estas directrices están recogidas en diversas guías publicadas por las autoridades competentes de Estados Unidos y definen las obligaciones de los bancos de mantener controles internos, sistemas de información apropiados al tamaño, naturaleza, alcance y riesgo de la institución, evaluaciones de los riesgos y procedimientos adecuados, disponer de sistemas de auditoría interna y obliga a implementar actividades que fortalezcan la seguridad, confidencialidad e integridad de la información del cliente. Estas guías comenzaron en agosto de 2023 a incluir, por orden de la FED, los cuatro requisitos más importantes para la gestión del riesgo operacional: gestión de notificación de incidentes, continuidad del negocio

y planificación, gestión de terceros y pruebas o revisiones de las medidas de gestión del riesgo operacional (pp 3-4).

A diferencia de DORA, en Estados Unidos cada una de las autoridades competentes tienen una función en cada uno de los requisitos previamente establecidos:

1.1. Gestión de notificación de incidentes

En caso de incidente o ciberataque y según la Junta de Gobernadores del Sistema de la Reserva Federal (2024), las instituciones financieras estadounidenses deben utilizar la *Computer-Security Incident Notification Rule* que requiere a los organizadores de los bancos notificar de las incidencias en no más de 36 horas después de haberse ocasionado la incidencia (pp 10). Una vez generada, los miembros de las autoridades competentes desarrollaran su función que en este caso, la FED supervisaría las notificaciones de los incidentes y coordinaría las respuestas en los bancos; la OCC exigiría reportes del incidente ocasionado y la FDIC trataría de asegurarse de que los bancos informen de eventos críticos.

1.2. Continuidad de negocio y planificación

El segundo requisito indicado por la Reserva Federal es que las entidades de crédito deben desarrollar planes de continuidad del negocio, así como planes de recuperación ante desastres, que garanticen la operativa de las mismas frente a cualquier tipo de interrupción de la actividad. La puesta en marcha de los planes en las entidades de crédito será objeto de supervisión por la Fed y servirá para hacer la coordinación de las respuestas de las distintas entidades bancarias a la vez que la OCC forzará a las entidades a reportar los incidentes y comprobar la efectividad de los planes de continuidad o planes de respuesta, mientras que la FDIC se asegurará que los bancos informen sobre los incidentes y desarrollen planes para mitigar el impacto de los mismos.

En este sentido es de destacar la importancia de la *Federal Reserve Operating*

Circular No 5 que obliga a las entidades a implantar controles técnicos, operacionales, de gestión y procedimientos con el objetivo de proteger la seguridad del ecosistema de las TIC usadas para el acceso a los servicios y aplicaciones del Reserve Bank.

1.3. Gestión de terceros

El tercer requisito que se establece por la FED para la consecución de una mejora en la ciberseguridad es la gestión de terceros mediante estrategias de supervisión de riesgos asociados a proveedores de servicios TIC (procesamiento de pagos, infraestructura en la nube y seguridad). Para ello, la FED se encarga de supervisar los riesgos que derivan de la contratación de este tipo de servicios, tratando de revisar que se realiza un cumplimiento de los estándares de seguridad de los bancos; la OCC regula la gestión de proveedores evaluando el tipo de contrato realizado para las externalizaciones y la FDIC establece y exige a los bancos auditorias de seguridad de los proveedores de servicios TIC para mitigar los riesgos asociados a los mismos.

1.4. Pruebas o revisiones de las medidas de gestión del riesgo operacional

En el cuarto requisito de la FED se establece que para verificar la eficacia de los controles de seguridad y resiliencia operativa de todas las entidades bancarias deben realizar previamente pruebas o evaluaciones mediante auditorías internas o simulaciones de ciberataques. En este sentido la Junta de Gobernadores del Sistema de la Reserva Federal establece que: “La Reserva Federal lleva a cabo exámenes y seguimiento de la gestión de riesgos de ciberseguridad, gobernanza y controles en las instituciones supervisadas. (…) El personal examinador de la Reserva Federal utiliza el Sistema de Calificación Uniforme para Tecnología de la Información (URSIT)”; la OCC por su parte supervisa la implementación de las pruebas en los bancos y realiza un análisis de los resultados para así poder fortalecer las estrategias de minimización de los riesgos cibernéticos y la FDIC verifica la eficiencia de los controles impulsados en los bancos y realiza recomendaciones de mejora en materia

de resiliencia operativa.

De esta manera, las regulaciones efectuadas por la Reserva Federal, la OCC y la FDIC reforzaron de forma muy importante la operativa de lo digital del sector financiero de los Estados Unidos en el año 2024; para poder asegurar la adopción de todas las citadas directrices para la gestión del riesgo cibernético, la notificación oportuna de incidentes, la planificación de continuidad del negocio, la gestión de los proveedores de servicios TIC y la práctica de las pruebas de seguridad de una manera más eficaz, ayudaron a las instituciones en una mejor capacidad de reacción frente a los ciberataques. En la medida en que el informe de la Junta de Gobernadores del Sistema de la Reserva Federal (2024) hace mención de las mejoras sustantivas que han observado las instituciones en su controles de seguridad y de lo altos porcentajes de conformidad de los mecanismos que se han llevado a cabo mediante el Sistema de Calificación Uniforme para Tecnología de la Información (URSIT) y, no obstante, a la frecuencia y a la pericia (en aumento) de los ciberataques, el sector ha sabido mantener la integridad y la disponibilidad de los servicios ayudando a la confianza del consumidor y contribuyendo a la estabilidad del sistema.

2. RESILIENCIA OPERATIVA DIGITAL EN REINO UNIDO

Al igual que todos los países relacionados, el tema de ciberseguridad se ha convertido en un tema de estado y en este sentido el Reino Unido ha tratado de no quedarse atrás, convirtiendo la resiliencia digital en una de las prioridades del Reino Unido por el uso generalizado en constante crecimiento que está teniendo la tecnología en la vida diaria y la aparición de nuevas amenazas en el ciberespacio. En este sentido, el gobierno británico pone de manifiesto hacer frente a las mismas con gran compromiso mediante la publicación de la Estrategia Nacional de Ciberseguridad 2022. La implementación de esta estrategia se apoya en la cantidad de £2.6bn de inversión pública entre 2022-2030, basándose la misma en tres pilares fundamentales: construir un Reino Unido cibernéticamente resiliente, desarrollarse como una potencia cibernética líder y moldear un mundo digital seguro (Cabinet Office, 2022).

Asimismo, dentro del ecosistema digital del sector financiero británico, el Banco de Inglaterra (BoE), la Financial Conduct Authority (FCA) y la Prudential Regulation Authority (PRA) han evidenciado que la creciente digitalización del sector se está convirtiendo en un aspecto crítico para el mismo. Estas tres autoridades han creado un marco regulador preciso con el fin de robustecer las competencias de las entidades financieras y así, evitar posibles fallos operativos. Asimismo, han desarrollado tres reglamentos fundamentales para entender y fortalecer el marco de la resiliencia operativa digital en Reino Unido: PS21/3 de la FCA, la SS1/21 de la PRA y la Declaración del Bank of England sobre la Supervisión de la Resiliencia Operativa. Con estas tres normativas se sustentan los tres pilares fundamentales: la identificación de servicios críticos (Important Business Units o IBS), la definición de tolerancias de impacto y las pruebas de resiliencia y mapeo de recursos.

2.1. Identificación de servicios críticos o IBS

La FCA define los IBS (Important Business Service) de la siguiente manera: "un servicio prestado por una empresa, o por otra persona en nombre de la empresa a uno o más clientes de la empresa que, de interrumpirse, podría (i) causar niveles intolerables de daño a uno o más clientes de la empresa; o (ii) suponer un riesgo para la solidez, estabilidad o resistencia del sistema financiero del Reino Unido o para el funcionamiento ordenado de los mercados financieros." Por orden de las autoridades competentes en Reino Unido, en la Normativa PS21/3 y la SS1/21 establecen que todas las entidades financieras deben identificar todos los servicios esenciales o IBS al menos una vez al año o en caso de grandes cambios ocasionados dentro de la entidad.

Bank of England & Prudential Regulation Authority (2022) establecen que la forma de identificar un servicio empresarialmente importante o IBS es analizando cómo impacta un evento crítico en ese servicio específico. A fin de identificar los IBS se deben cumplimentar los siguientes criterios:

- Riesgo de disrupción y su impacto en la estabilidad financiera
- Solidez de la entidad

- Protección de titulares de pólizas en caso de aseguradoras

Esto significa que las entidades financieras son obligadas a identificar aquellos servicios cuyo riesgo tenga un impacto directo en el funcionamiento de la economía y el sistema financiero de Reino Unido, el impacto que ha ocasionado esta disrupción en la entidad o firma, ayudando a establecer cómo y porqué se ha actuado de esa forma y por último, el impacto en la seguridad de los clientes y la protección de la información personal y privada de los mismos.

2.2. Tolerancia al Impacto

Una vez identificados los servicios empresariales importantes (IBS), por orden de la PRA se establece lo siguiente:

> "exige a las empresas que fijen una tolerancia de impacto para cada uno de sus servicios empresariales importantes. Las Partes de Resiliencia Operativa definen una tolerancia de impacto como el nivel máximo tolerable de interrupción de un IBS, medido por una duración de tiempo, además de cualquier otro parámetro pertinente."

Es decir, para cada servicio critico definir un límite máximo de tiempo o grado de disrupción que ese servicio pueda soportar sin que se produzcan grandes inconveniencias.

Financial Conduct Authority (2021) indica que no hay una definición exacta sobre un daño intolerable debido a que los parámetros o métricas que se deban incluir en los planes de las empresas varían en función de la actividad que se desarrolle en cada una de ellas. En consonancia con la PRA, la FCA (2021) establece posibles factores que puedan ser considerados intolerables como pérdidas financieras para el consumidor o empresa, propagación de riesgos a otros servicios empresariales o al sistema financiero británico, número y tipos de consumidores afectados junto con la naturaleza del impacto, pérdida de funcionalidad, etc…

En este sentido, Bank of England & Prudential Regulatory Authority (2022) ha establecido tres requerimientos clave que las entidades deben cumplir para poder

hacer frente de forma más efectiva a las amenazas cibernéticas que afectan al sector financiero:

1. Las entidades están obligadas a documentar e informar de las tolerancias al impacto a la PRA, de forma que haya una supervisión efectiva por parte de las autoridades competentes y garantiza una gestión de riesgos sistémicos de carácter preventivo para asegurar la estabilidad del sistema financiero británico.
2. Revisión periódica de incidentes que superan la tolerancia de impacto determinado previamente. De esta forma, se renuevan y se adaptan a los cambios que ocurran en la estructura del sector o de la propia entidad.
3. Realización de pruebas de estrés para probar que las entidades pueden funcionar bajo los límites establecidos en la tolerancia al impacto. Mediante las pruebas o simulaciones de incidentes, ensayan unos escenarios que les permiten determinar y analizar cómo es el funcionamiento y la resistencia de la entidad en el caso de operar frente a eventos extremos o críticos.

2.3. Pruebas de resiliencia o mapeo de recursos

El tercer pilar fundamental de la resiliencia operativa en el sector bancario británico es el mapeo de recursos o *mapping*. Según SS1/21 de la PRA se define este concepto como la identificación y documentación de los recursos clave que son necesarios para desarrollar las actividades de las IBS con el fin de interceptar las vulnerabilidades en caso de la falta de los recursos esenciales y la capacidad de permanecer bajo los límites de tolerancias al impacto establecidos dentro de las IBS. Los recursos que deben ser mapeados por cada IBS y a los que esta normativa se refiere son:

- **Personas** esenciales para las operaciones de las entidades financieras como equipos de soporte tecnológico o de ciberseguridad y responsables de operaciones bancarias y gestión de crisis
- **Procesos** internos críticos, es decir, aquellos procesos internos que son esenciales para el desarrollo de las IBS

- **Infraestructura tecnológica** disponible por las entidades financieras y las dependencias externas o proveedores de servicios TIC como redes de pago y liquidación, software financiero, computación en la nube…
- **Instalaciones** o recursos físicos como las oficinas o sucursales
- **Información** clave de los clientes, empleados o proveedores que requieren unos protocolos de protección de datos y una gestión muy eficiente de la seguridad de la información

La identificación de estos recursos y el mapeo de los mismos permite a las entidades comprender las situaciones extremas desde un punto de vista preventivo y garantiza que las entidades desarrollen planes de contingencia para así poder mitigar todos los riesgos provenientes de los incidentes de forma estratégica.

Según Bank of England (2024) en la actualidad, la resiliencia operativa digital en el Reino Unido ha mostrado evoluciones favorables en la gestión de la ciberseguridad al transitar 2024, principalmente por aplicación de la Estrategia Nacional de Ciberseguridad 2022. Este enfoque ha determinado que se haya creado una iniciativa apropiada para la gestión de las ciber amenazas, de modo que la ciberseguridad se haya convertido en un elemento destacado en favor de la estabilidad económica del país y de su seguridad nacional.

Los resultados de las pruebas de estrés realizadas durante 2024 evidencian que la banca británica posee la capacidad de hacer frente a condiciones económicas adversas, asumiendo cotas de capital por encima de los umbrales mínimos. Esto implica que las capacidades que hayan sido implementadas de forma activa han sido útiles, tanto para los riesgos en sí como para las instituciones a la hora de poder hacer frente a situaciones de interrupción operativa. Además, la determinación de los servicios críticos y el mapeo de los recursos cuenta con un valor en la investigación de las capacidades que ayudan a conocer el conjunto de vulnerabilidades y los planes de contingencia de soporte, pudiendo operar dentro de los márgenes de tolerancia al impacto detectados. No obstante, aún a pesar de que se han alcanzado estos avances, sigue siendo necesario que las autoridades y las instituciones continuen con la detección de riesgos y la adaptación de la respuesta que deben ofrecer para hacer frente a todo lo que se pueda presentar en ciberespacio.

3. COMPARATIVA INTERNACIONAL: EE.UU vs REINO UNIDO vs UNION EUROPEA

En respuesta a los desafíos de un mundo cada vez más digitalizado, diferentes jurisdicciones han desarrollado marcos regulatorios que refuerzan las habilidades de las entidades financieras para detectar, prevenir y soportar los fallos que ocurren en la operatividad de las mismas. En este apartado, se presentarán la comparativa con los enfoques dados por las autoridades financieras de Reino Unido, Estados Unidos y la Unión Europea (DORA). El análisis estará basado en la comparación de los factores como las autoridades competentes y sus funciones, el marco regulatorio, el enfoque y las diferencias que existen en materia de los cuatro pilares fundamentales para la resiliencia digital en el sector bancario, ya que, en aspectos generales, en las tres jurisdicciones son incluidos: gestión del riesgo tecnológico, gestión de terceros, pruebas de resiliencia y notificación de incidentes.

3.1. Autoridades competentes

Por autoridades competentes entendemos aquellas instituciones financieras que se encargan de supervisar y de regular las actividades del sector bancario garantizando la estabilidad y transparencia del sistema. Para cada uno de los países mencionados en este apartado, la implementación de normativas que fortalecen la resiliencia digital de las entidades han sido lideradas por autoridades o agentes financieros que han desempeñado un papel de control y supervisión para el correcto funcionamiento de las mismas.

Unión Europea

En Europa, según el Parlamento Europeo y Consejo de la Unión Europea (2022), las autoridades competentes con responsabilidad en la supervisión de DORA son aquellas que tengan competencias a nivel nacional y en materia financiera y tecnológica.

En el caso de España, la autoridad supervisora y a la que las entidades financieras

españolas deben reportar es el Banco de España, cuya fecha límite de implementación en el territorio es del 17 de enero de 2025.

Reino Unido

El marco de resiliencia operativa está liderado en Reino Unido por el Banco de Inglaterra (BoE) junto con la Prudential Regulation Authority (PRA), son entidades reguladoras y supervisora que trabajan mano a mano para conseguir la estabilidad financiera del país. Éstas emiten los estándares y reglamentos de obligado cumplimiento que garanticen un correcto funcionamiento de las entidades financieras cuando se encuentren en eventos críticos o disruptivos y obliga a éstas a cumplir con los requisitos establecidos.

Además, hay otra autoridad financiera británica la Financial Conduct Authority (FCA) cuya función es: "Nosotros trabajamos para asegurar que los mercados trabajan bien para los individuos, empresas y por el crecimiento y competitividad de la economía de Reino Unido". Con respecto a la resiliencia operativa digital, la FCA se encarga de asegurar que las entidades financieras cumplen con lo establecido por el BoE y la PRA para así cumplir con el objetivo definido.

Estados Unidos

La regulación de la resiliencia operativa en Estados Unidos está dividida en tres agencias diferentes. En primer lugar, la Federal Reserve (Fed) cuya función es supervisar que la seguridad cibernética en los bancos a nivel global es fuerte y colabora con ellos para mejorar la capacidad de estos de hacer frente a los eventos a los que se tenga que enfrentar el sector financiero. En segundo lugar, la Office of the Comptroller of the Currency (OCC) que se encarga de regular y supervisar los bancos nacionales, por tanto, se encarga de verificar la correcta implantación de las normativas emitidas por la Fed en materia de resiliencia digital. Y, por último, la Federal Deposit Insurance Corporation (FDIC) que asegura los depósitos y supervisa que las entidades financieras pueden proteger al consumidor. En el caso de la resiliencia digital, uno de los objetivos primordiales es evitar que los consumidores se vean afectados por un evento que interrumpa la actividad de las

entidades bancarias.

TABLA 1. Comparativa Autoridades Competentes

	Unión Europea	**Reino Unido**	**Estados Unidos**
Autoridades competentes	- Banco Central Europeo (BCE) - Bancos Centrales Nacionales (ej: Banco de España)	- Bank of England - Prudential Regulation Authority (PRA) - Financial Conduct Authority (FCA)	- Federal Reserve - Office of the Comptroller of the Currency (OCC) - Federal Deposit Insurance Corporation (FDIC)

3.2. Marco Regulatorio

El marco regulatorio son las leyes o reglamentos aplicados al sector financiero. En este análisis se identifican cuáles son las normativos y reglamentos por región estudiada.

Unión Europea

La Digital Operational Resilience Act (DORA) es el reglamento emitido por el Banco Central Europeo que busca homogeneizar la aplicación de la regulación en todo el territorio de la Unión Europea, consiguiendo así, que todas las entidades financieras puedan cumplir con unos requisitos básicos y uniformes en materia de resiliencia digital.

Reino Unido

El marco regulatorio de Reino Unido está compuesto por dos normativas principales: la Normativa PS21/3 y la SS1/21.

Por un lado, la SS1/21 fue emitida por la Prudential Regulation Authority (PRA)

para mejorar habilidad de las entidades financieras de ser más resilientes desde el punto de vista tecnológico. De esta manera, se centra en garantizar la estabilidad y seguridad del sistema financiero.

Por otro lado, la PS21/3 está basada en los estándares de la SS1/21 y amplia la aplicación de la normativa a otras entidades financieras para poder proteger al consumidor frente a incidentes tecnológicos y para así favorecer a una mayor estabilidad del mercado británico.

Estados Unidos

En Estados Unidos, cada autoridad publicó una guía o informe que permitía comprender paso a paso la implantación de la resiliencia digital en el sector financiero estadounidense.

Por un lado, la Fed emitió el *Cybersecurity and financial system resilience report* que define los requisitos necesarios sobre la ciber resiliencia para ser implantados en las entidades financieras estadounidenses.

Por otro lado, la OCC también publicó una guía *Sound Practices to Strengthen Operational Resilience* que respalda los requisitos establecidos por la Fed para hacer frente a las amenazas digitales del sistema financiero y permite conocer de forma detallada los puntos más importantes para la implementación de estas prácticas.

TABLA 2. Comparativa Marco Regulatorio

	Unión Europea	**Reino Unido**	**Estados Unidos**
Marco Regulatorio	Digital Operational Resilience Act (DORA)	- PS21/3 - SS1/21	- Cybersecurity and financial system resilience report. - Sound Practices to Strengthen Operational Resilience

3.3. Enfoque

Unión Europea

La Unión europea concentra su regulación no sólo en el cumplimiento de DORA por parte de las entidades financieras, sino que también incluye requisitos exhaustivos y una tarea de revisión para los proveedores de los servicios TIC.

Reino Unido

Reino Unido en algunos aspectos del enfoque se puede establecer que es similar al de la Unión Europea debido a la Declaración sobre la cooperación supervisora en la resiliencia operativa (2020) donde insiste en la cooperación con otras autoridades financieras para alinear los objetivos de gestión de la resiliencia digital a nivel global. Debido a la proximidad territorial con Europa, Reino Unido ha tratado de tomar ciertas notas de DORA para aplicar en su marco regulatorio. No obstante, las normativas individuales emitidas por el Banco de Inglaterra están principalmente enfocadas en la actividad de "Tolerancia al Impacto" que, como explicado anteriormente, es el nivel máximo de tiempo o grado de disrupción que una entidad puede tolerar antes de que se vuelva una amenaza para la misma.

Estados Unidos

El marco europeo y estadonidense comparten una mayoría de principios y requisitos, como el principio de proporcionalidad [3]y coincide con tres de los cuatro puntos principales de la regulación: gestión de notificacion de incidentes, gestión de terceros y las pruebas de estrés o de las medidas implantadas en materia del riesgo operacional. No obstante, el marco norteamericano está muy centrado en la ciberseguridad y en la revisión constante de todos los riesgos operativos que puedan impactar en las actividades desarrolladas por las entidades financieras.

[3] Reglamento DORA, Artículo 4: "Las entidades financieras aplicarán las normas establecidas en el Capítulo II de conformidad con el principio de proporcionalidad, teniendo en cuenta su tamaño y perfil de riesgo general, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones."

TABLA 3 Comparativa del enfoque de la normativa

	Unión Europea	**Reino Unido**	**Estados Unidos**
Enfoque	Gestión de proveedores TIC	Impact Tolerances o Tolerancia al Impacto	Ciberseguridad y poca homogeneidad.

TABLA 4. Comparativa Internacional: UE vs UK vs US

	Unión Europea	Reino Unido	Estados Unidos
Autoridades Competentes	Banco Central Europeo y a nivel local, autoridades nacionales (ej: Banco de España)	Bank of England, Prudential Regulation Authority (PRA) y Financial Conduct Authority (FCA).	Federal Reserve (Fed), OCC (Office of the Comptroller of the Currency y FDIC (Federal Deposit Insurance Corporation)
Marco Regulatorio	Digital Operational Resiliencia Act (DORA) con el objetivo homogeneizador en términos regulatorios.	Operational Resilience: Impact tolerances for important business services (SS1/21) y Building operational resilience: Feedback to CP19/32 and final rules (PS21/3).	Cybersecurity and financial system resilience report, Interagency Guidelines Establishing Information Security Standards y Sound Practices to Strengthen Operational Resilience.
Enfoque	Centrado en la gestión de proveedores de servicios TIC.	Centro de la regulación basado en los "Impact Tolerances" o Tolerancia al impacto.	Enfocado en la ciberseguridad del sector financiero, pero poca homogeneización
Requisitos o principios	• Gestión y gobernanza del riesgo de TIC • Notificacion de incidentes (no más de 24 horas) • Pruebas de resiliciencia • Gestion del riesgo con terceros	• Identificación de las IBS • Tolerancia al impacto • Pruebas de resiliencia o mapeo de recursos	• Gestión de notificacion de incidentes (no más de 36 horas) • Continuidad del negocio y planificación • Gestión de Terceros • Pruebas o revisiones de las medidas de gestión.

CAPITULO V. CONCLUSIONES

En esta sección se destacan las diferentes conclusiones que se han extraído a lo largo de este trabajo.

En primer lugar, se pueden establecer las siguientes conclusiones generales del entorno bancario o sector financiero actual:

1. Riesgos no financieros que generan gran preocupación en el sector son: riesgos tecnológicos, riesgos operacionales y el riesgo de externalizaciones. Siendo el cibernético el más preocupante.
2. El impacto reputacional y operativo de incidentes provenientes de los riesgos mencionado previamente, pueden dañar la confianza del cliente y la estabilidad financiera.
3. Surgimiento de normativa DORA en el cuadro europeo para fortalecer la resiliencia digital y mitigar los riesgos derivados de las externalizaciones y la tecnología como los ciberataques.

En segundo lugar, se realiza un estudio comparativo de las normativas dedicadas a la resiliencia operativa digital a nivel internacional en los marcos europeos, estadounidenses y británicas. Se obtienen las siguientes conclusiones:

1. La Unión Europea, con la introducción de DORA, adopta en cambio un marco regulatorio más centralizado, homogeneizado, de manera que la regulación es aplicable a todos los actores que tengan en su mano los servicios de tecnología de la información, de forma que también tiene requerimientos de custodio para los incidentes relacionados con la resiliencia y la propia gestión del riesgo de los proveedores de servicios TIC.
2. El caso del Reino Unido, que tras el Brexit no es ya parte de la UE, presenta un mecanismo que adopta algunas prácticas de legislaciones similares dentro de su marco, como la PS21/3 y SS1/21 priorizando en este caso las "Impact Tolerances", es decir, el umbral de disrupción que una entidad puede permitir antes de verse comprometida como entidad para continuar dando servicio.

3. En Estados Unidos, el marco regulador se presenta más desestructurado y fragmentado cuyas funciones se ven divididas entre varias agencias (Fed, OCC, FDIC), lo que aporta mayor flexibilidad pero con una menor homogeneización en comparación con la UE. La regulación también hace hincapié en la ciberseguridad, presentando documentos como el "Cybersecurity and Financial System Resilience Report", que junto con el "Sound Practices to Strengthen Operational Resilience" quieren reforzar la capacidad de las entidades para enfrentar las amenazas específicas de los entornos digitales.
4. Si bien los enfoques y marcos regulatorios son distintos, todos ellos coinciden en cuatro pilares básicos: gestión del riesgo tecnológico, supervisión de terceros, pruebas de resistencia y notificación de incidentes, lo que apoya el interés expreso a nivel internacional de reforzar la estabilidad y seguridad del sistema financiero en un contexto cada vez más digitalizado.

En resumen, la resiliencia operativa en el sector bancario es una de las bases más importantes en todos los procesos en los que se hace necesaria la buena estabilidad de la finanza internacional, y cada una de las jurisdicciones ha ido desarrollando sus propios marcos regulatorios según las necesidades y finanzas de cada uno.

En tercer lugar, se incluyen mis propias conclusiones del estudio en base a las diferencias clave entre las normativas y las respuestas que pueden dar las entidades financieras en base a la exigencia de éstas:

1. DORA supone el marco más completo y normativamente más exigente del analizado. Establece obligaciones muy exhaustivas que van desde la descripción de las estructuras internas de gobernanza hasta requisitos técnicos que giran en torno a pruebas de penetración, clasificación de incidentes o cláusulas contractuales de obligada inclusión en los acuerdos con proveedores TIC. Este grado de análisis y diagnostico asegura niveles altos de seguridad, pero también puede acarrear una elevada carga de cumplimiento, en especial para las entidades medianas y pequeñas.
2. Reino Unido con la presentación de un marco estructurado y un poco más flexible con una regulación basada en el concepto de la Tolerancia al Impacto, permite a las entidades financieras ajustar estos controles a las

capacidades de la misma. Esta flexibilidad puede convertirse en una característica atractiva para las entidades y valorar su instalación en un marco como éste.

3. En Estados Unidos, la fragmentación y división de funciones entre diferentes agencias (Fed, OCC y FDIC) permite dar más flexibilidad que en Reino Unido y no se limita a un marco común como en la UE con DORA. Esta libertad de aplicación permite a los supervisores tener una interpretación subjetiva de la normativa generando inestabilidad en términos regulatorios dentro de un mismo territorio.

En definitiva, con este análisis comparativo se puede determinar de forma estratégica la instalación geográfica de una entidad cuando se trata de criterios regulatorios. Por tanto, en un futuro no muy lejano, en un sector financiero cambiante y cada vez más digitalizado, el factor de la localización de las entidades podrá ser establecido en base a la exigencia y apoyo institucional al marco normativo vigente en el país de destino.

CAPITULO VI. PROYECCIONES FUTURAS DE LA RESILIENCIA DIGITAL

Tras haber realizado este estudio, se puede establecer que la resiliencia digital se está comenzando a consolidar como el centro de la estabilidad financiera internacional debido a la evolución de las amenazas que acechan a este sector como la tecnología y ciberataques. En este sentido, las instituciones financieras considero que deberán mantenerse actualizadas de dichas evoluciones y adaptarse de forma continua para mitigar los riesgos derivados de ellas. Por tanto, es importante predecir o proyectar posibilidades del desarrollo de la resiliencia digital en este sector en los próximos años:

1. **Armonización normativa o regulatoria**. A pesar de las diferencias que existen entre las normativas, tienen unos requisitos comunes que permitirán la creación de estándares generales para una aplicación unificada en todo el sector financiero, fomentando así la cooperatividad internacional en materia regulatoria.

2. **Utilización de la Inteligencia Artificial (IA) como herramienta para la supervisión y la prevención.** Actualmente, la Inteligencia Artificial ha trasformado por completo el ecosistema digital permitiendo incorporar tecnologías predictivas mucho más precisas. Por ello, las entidades financieras podrían hacer uso de modelos IA para anticiparse a amenazas cibernéticas o identificar irregularidades de sistemas tecnológicos de forma mucho más eficiente. Además, podrá controlar el cumplimiento normativo de una manera más rigurosa analizando riesgos y mejorando la capacidad de respuesta.

3. **Normativas o marcos regulatorios como criterio para localización de entidades financieras**. La dureza y exigencia de cada normativa se convertirá en un criterio en toma de decisiones con un carácter estratégico en las entidades financieras dado que preferirán ajustarse a aquellas normativas que sean más convenientes para ellas, desde el punto de vista empresarial.

4. **Crecimiento de nuevas amenazas (también por IA).** En este contexto, volverán a surgir otros ataques de ciberseguridad cada vez más complejos y peligrosos. Esto forzará a las entidades financieras a fortalecer, no solo los modelos de resiliencia digital, sino a proteger de forma más eficaz todo el ecosistema financiero en sí.

   La IA puede ser un factor de riesgo fundamental, debido a que si se realizase una mala praxis de ésta como diseños de ciberataque más sofisticado de los ya existentes, podría tener consecuencias graves para las entidades financieras.

5. **Resiliencia digital como cultura empresarial.** El evidente aumento de los ataques a las entidades financieras las ha obligado a implantar normativas como DORA para protegerse frente a estos ataques y mitigar los riesgos operacionales. Sin embargo, en un contexto a largo plazo, la resiliencia digital se convertirá en parte de la cultura organizacional de las entidades financieras, posiblemente integrando indicadores que permitirán medir el rendimiento de las entidades en este sentido o implementando prácticas dirigidas a combatir los ciberataques como parte de un plan directivo.

En conclusión, considero que los puntos desarrollados en este capítulo pueden ser la continuación de este estudio debido a que la resiliencia operativa digital en el sector financiero no será combatida únicamente con normativas como las estudiadas en este trabajo, sino que se verá desafiada en múltiples ocasiones por un entorno cambiante y en constante evolución tecnológica.

CAPITULO VII. DECLARACION SOBRE EL USO DE CHATGPT U OTRAS HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL

Por la presente, yo, Andrea María García García, estudiante de E-2 en Inglés de la Universidad Pontificia Comillas al presentar mi Trabajo Fin de Grado titulado "Resiliencia Digital en el Sector Financiero: Un análisis Comparativo de DORA y su impacto en el Riesgo Operacional a Nivel Internacional" declaro que he utilizado la herramienta de Inteligencia Artificial Generativa ChatGPT u otras similares de IAG de código sólo en el contexto de las actividades descritas a continuación:

1. **Brainstorming de ideas de investigación:** Utilizado para idear y esbozar posibles áreas de investigación.

2. **Referencias:** Usado conjuntamente con otras herramientas, como Science, para identificar referencias preliminares que luego he contrastado y validado.

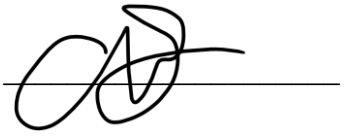
3. **Corrector de estilo literario y de lenguaje:** Para mejorar la calidad lingüística y estilística del texto.

4. **Sintetizador y divulgador de libros complicados:** Para resumir y comprender literatura compleja.

5. **Revisor:** Para recibir sugerencias sobre cómo mejorar y perfeccionar el trabajo con diferentes niveles de exigencia.

Afirmo que toda la información y contenido presentados en este trabajo son producto de mi investigación y esfuerzo individual, excepto donde se ha indicado lo contrario y se han dado los créditos correspondientes (he incluido las referencias adecuadas en el TFG y he explicitado para que se ha usado ChatGPT u otras herramientas similares). Soy consciente de las implicaciones académicas y éticas de presentar un trabajo no original y acepto las consecuencias de cualquier violación a esta declaración.

Fecha: 26 de Marzo de 2025.

Firma: 

CAPITULO VIII. BIBLIOGRAFÍA

ABC. (2024, 14 de mayo). *El Banco Santander sufre un hackeo en España, Chile y Uruguay*. ABC.

APTE (2024). Informe De Situación 2024 sobre Cyberseguridad. Ediciones Disruptivas.

Autoridad Bancaria Europea. (2024). *EBA Risk Assessment Questionnaire 2024*. European Banking Authority. https://www.eba.europa.eu/

Banco de España. (2006). *Riesgo operacional. Banco de España*. Recuperado de https://www.bde.es/f/webbde/Agenda/Eventos/06/Nov/Fic/10_II_Seminario_BII_MAN-IGF_RO.pdf

Bank of England. (2020). *Statement Regarding supervisory cooperation on operational resilience.* Recuperado de: https://www.bankofengland.co.uk/prudential-regulation/publication/2020/statement-regarding-supervisory-cooperation-on-operational-resilience

Bank of England. (2024). *Financial stability report: November 2024*. Recuperado de: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability-report/2024/financial-stability-report-november-2024.pdf

Bank of England, Prudential Regulation Authority. (2022). *Operational Resilience: Impact tolerances for important business services (SS1/21).* Recuperado de: https://bit.ly/41u1SG5

Bamber, P., & Fernández-Stark, K. (2022). North America in Global Value Chains. Duke University, Global Value Chains Center. Recuperado de https://bit.ly/3RaPZjw

BIS. **Bank for International Settlements** (2023). Annual Report 2023.

Board of Governors of the Federal Reserve System. (2024). *Cybersecurity and financial system resilience report*. Recuperado de https://www.federalreserve.gov/publications/files/cybersecurity-report-202407.pdf

Cabinet Office. (2022). *National Cyber Security Strategy 2022-2030*. GOV.UK. Recuperado de https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030

Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, Materne S. *Cyber risk and cybersecurity: a systematic review of data availability*. Geneva Pap Risk Insur Issues Pract. 2022;47(3):698-736. doi: 10.1057/s41288-022-00266-6. Epub 2022 Feb 17. PMID: 35194352; PMCID: PMC8853293.

CTI-TEND. (2024). *Informe de tendencias y ciberamenazas del 1er semestre de 2024*. Departamento de Cyber Threat Intelligence de NTT DATA Cybersecurity.

ECB. (2020). Cyber resilience for financial institutions

Federal Deposit Insurance Corporation (FDIC). (s.f). *Acerca de la FDIC*. Recuperado de: https://www.fdic.gov/espanol/acerca-de-la-fdic

Federal Deposit Insurance Corporation (FDIC). (2024). *Interagency Guidelines Establishing Information Security Standards*. Recuperado de https://www.fdic.gov.

Federal Reserve Banks. (2024). *Operating Circular 5: Electronic access.* Federal Reserve Financial Services. Recuperado de: https://bit.ly/43QNpXn

Financial Conduct Authority. *About the FCA*. Recuperado de: https://www.fca.org.uk/about/what-we-do/the-fca

Financial Conduct Authority. (2021). *Building operational resilience: Feedback to CP19/32 and final rules (PS21/3)*. Recuperado de: https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf

Funcas. (2024). Ciberriesgo en el sector bancario europeo. Funcas. Recuperado de https://www.funcas.es/odf/ciberriesgo-en-el-sector-bancario-europeo/

Infordisa. (2024, Mayo 14). Filtración masiva de datos del Banco Santander. https://www.infordisa.com/soc/filtracion-masiva-de-datos-del-banco-santander/

KPMG. Benchmark de riesgos no financieros. KPMG España, noviembre de 2022. https://kpmg.com/es/es/informes-publicaciones/2022/11/benchmark-riesgos-no-financieros.html.

KPMG Tendencias. (2018). Externalización en la banca: el foco del BCE. Recuperado de https://www.tendencias.kpmg.es/2018/06/externalizacion-banca-bce/

Marsh. (2022). What is cyber risk? Marsh. Recuperado de https://www.marsh.com/co/services/cyber-risk/insights/what-is-cyber-risk.html

Office of the Comptroller of the Currency. (2024). *Cybersecurity and financial system resilience: 2024 report*. Recuperado de: https://www.occ.treas.gov/publications-and-resources/publications/cybersecurity-and-financial-system-resilience/files/pub-2024-cybersecurity-report.pdf

Office of the Comptroller of the Currency (OCC), Federal Reserves & Federal Deposit Insurance Corporation. (2020). *Sound Practices to Strengthen Operational Resilience*. Recuperado de https://www.federalreserve.gov

Peláez, J. (2024). El reglamento DORA. Informe de INCIBE.

Parlamento Europeo y Consejo de la Unión Europea. (2022). Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012 y (UE) n.º 600/2014. Diario Oficial de la Unión Europea, L 333, 27.12.2022, pp. 1-79

Revista RUE. (2024). Plan de continuidad del negocio y riesgo operacional y financiero. Revista RUE (n.º 6, 2024). Recuperado de https://revistarue.eu/RUE/062024.pdf