

**DERECHO MERCANTIL**



**La Ley Europea de Resiliencia  
Operativa Digital del Sector Financiero  
El Reglamento (UE) 2022/2554  
(DORA)**

**Alberto J. Tapia Hermida**

*Catedrático de Derecho Mercantil  
Universidad Complutense de Madrid*

**REUS**  
EDITORIAL

# COLECCIÓN DE DERECHO MERCANTIL

## TÍTULOS PUBLICADOS

- Conflicto de intereses y comisión mercantil**, *Elena Leñena Mendizábal* (2009).
- El acceso a la condición de socio en la sociedad cooperativa de trabajo asociado**, *Pedro J. Lassaletta García* (2010).
- El contrato de permuta comercial (BARTER)**, *José Antonio Vega Vega* (2011).
- Apertura de grandes superficies comerciales y libertades comunitarias**, *Eduardo Estrada Alonso, Raúl I. Rodríguez Magdaleno, Ignacio Fernández Chacón* (2011).
- Sociedades Anónimas Deportivas. Régimen jurídico actual**, *Isabel Ramos Herranz* (2012).
- Derecho Mercantil Electrónico**, *José Antonio Vega Vega* (2015).
- El contrato de obra por empresa**, *Antonio Tapia Hermida* (2016).
- Aprovisionamiento y stock en los contratos de distribución integrada**, *Pablo Jarne Muñoz* (2016).
- Régimen jurídico de los autónomos. Aspectos mercantiles, administrativos laborales y fiscales**, *José Antonio Vega Vega (Dir.)* (2018).
- Economía colaborativa y plataformas digitales**, *Pablo Jarne Muñoz* (2019).
- La empresa social en España e Italia**, *José Antonio Vega Vega (Coord.)* (2020).
- Introducción al Derecho Mercantil**, *José Antonio Vega Vega (Dir.)* (2020).
- Introducción al Derecho Mercantil (2.ª edición)**, *José Antonio Vega Vega (Dir.)* (2021).
- La protección del consumidor en el comercio electrónico transfronterizo**, *Marcial Herrero Jiménez* (2021).
- Introducción al Derecho Mercantil (3.ª edición)**, *José Antonio Vega Vega (Dir.)* (2022).
- Introducción al Derecho Mercantil (4.ª edición)**, *José Antonio Vega Vega (Dir.)* (2023).
- La nueva sociedad de responsabilidad limitada**, *José Antonio Vega Vega* (2024).
- Leyes Europeas de Mercados y de Servicios Digitales**, *Alberto J. Tapia Hermida* (2025).
- La Ley Europea de los Mercados de Criptoactivos (MiCA) y las criptomonedas**, *Alberto J. Tapia Hermida* (2025).
- La Ley Europea de Resiliencia Operativa Digital del Sector Financiero. El Reglamento (UE) 2022/2554 (DORA)**, *Alberto J. Tapia Hermida* (2025).

COLECCIÓN DE DERECHO MERCANTIL

Director:

ALBERTO J. TAPIA HERMIDA

Catedrático de Derecho Mercantil  
Universidad Complutense de Madrid

**La Ley Europea de Resiliencia  
Operativa Digital  
del Sector Financiero  
El Reglamento (UE) 2022/2554  
(DORA)**

Alberto J. Tapia Hermida

*Catedrático de Derecho Mercantil  
Universidad Complutense de Madrid*

**REUS**  
EDITORIAL

Madrid, 2025

© Alberto J. Tapia Hermida  
© Editorial Reus, S. A.  
C/ Aviador Zorita, 4, -2º B – 28020 Madrid  
Teléfonos (34) 91 521 36 19 – (34) 91 522 30 54  
Fax (34) 91 445 11 26  
reus@editorialreus.es  
www.editorialreus.es

1ª edición REUS, S.A. (2025)  
ISBN: 978-84-290-2972-7  
Depósito Legal: M-21451-2025  
Diseño de portada: Lapor  
Impreso en España  
Printed in Spain

Imprime: *Estugraf Impresores S.L.*

Ni Editorial Reus ni sus directores de colección responden del contenido de los textos impresos, cuya originalidad garantizan sus propios autores. Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra sólo puede ser realizada con la autorización expresa de Editorial Reus, salvo excepción prevista por la ley. Fotocopiar o reproducir ilegalmente la presente obra es un delito castigado con cárcel en el vigente Código penal español.

# ÍNDICE

ABREVIATURAS .....	5
PRESENTACIÓN .....	7
CAPÍTULO 1	
ASPECTOS GENERALES .....	13
I. ÁMBITO DE APLICACIÓN INTERNO Y EXTERNO.....	13
A) Ámbito interno .....	13
B) Ámbito externo .....	14
II. VIGENCIA.....	14
III. CONTEXTO NORMATIVO .....	15
A) La inserción de DORA en el Paquete Europeo de Finanzas Digitales .....	15
B) La complementariedad de DORA con el sistema de gestión del riesgo de las entidades financieras basado en el capital .....	16
C) La supletoriedad del DORA .....	17
1. Genérica .....	17
2. Específica .....	17

IV. CARACTERÍSTICAS DE DORA.....	18
A) El carácter directamente vinculante de DORA..	18
B) La proporcionalidad en la aplicación del DORA .....	19
V. CONTEXTO ECONÓMICO: LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC).....	19
CAPÍTULO 2	
ESTRUCTURA DEL DORA .....	23
I. ELEMENTOS SUBJETIVOS: LAS ENTIDADES FINANCIERAS .....	
A) Entidades financieras incluidas .....	23
1. Entidades del mercado bancario .....	24
2. Entidades del mercado de valores.....	24
3. Entidades del mercado de seguros .....	25
4. Entidades transversales a los tres sectores del mercado financiero .....	26
B) Entidades financieras excluidas.....	27
II. ELEMENTOS OBJETIVOS: RIESGO, INCIDENTE Y RESILIENCIA .....	
A) El riesgo.....	28
B) El incidente .....	30
C) La resiliencia .....	31
CAPÍTULO 3	
FUNCIONAMIENTO DEL DORA .....	33
I. LA GESTIÓN DEL RIESGO OPERATIVO DIGITAL .....	
A) El subsistema de gestión del riesgo operativo digital como parte del sistema global de gestión de riesgos de las entidades financieras .....	33

B) El establecimiento de un marco de gestión del riesgo operativo digital relacionado con las TIC	34
1. Requisitos de calidad del marco de gestión del ROD: adecuación, fiabilidad, capacidad y resiliencia .....	35
2. Requisitos de cantidad o contenido del marco de gestión del ROD: estrategias, políticas, procedimientos, y protocolos y herramientas .....	36
C) Gobernanza y control del marco interno de gestión del ROD por el órgano de dirección de la entidad financiera .....	38
D) Ejecución del marco de gestión del ROD.....	39
1. La protección y prevención.....	39
2. La detección de actividades anómalas .....	39
3. Respuesta y recuperación.....	39
4. Aprendizaje y evolución.....	40
5. Comunicación.....	40
<b>II. LA PREVENCIÓN DEL INCIDENTE OPERATIVO DIGITAL: LAS PRUEBAS DE RESILIENCIA OPERATIVA DIGITAL .....</b>	<b>41</b>
A) Programas de pruebas .....	41
1. Requisitos objetivos de las pruebas normales y avanzadas .....	42
a) Pruebas normales .....	42
b) Pruebas avanzadas.....	42
2. Requisitos subjetivos de los probadores externos e internos.....	43
a) Probadores externos .....	43
b) Probadores internos .....	44
B) Pruebas de penetración basadas en amenazas: El Reglamento Delegado 2025/1190 de la Comisión Europea .....	44
1. Aspectos generales .....	44

2. Ámbito de aplicación: entidades financieras obligadas a realizar pruebas de penetración basadas en amenazas .....	46
a) Los criterios de selección.....	47
b) Los tipos de entidades financieras seleccionadas.....	47
3. Gestión de las pruebas de penetración basadas en amenazas .....	48
a) Las autoridades competentes: los equipos de ciberseguridad y los gestores de pruebas de penetración basadas en amenazas .....	48
b) Las entidades financieras seleccionadas: sus disposiciones organizativas...	49
c) La gestión de riesgos de las pruebas de penetración basadas en amenazas .....	52
4. Cronología de las pruebas de penetración basadas en amenazas .....	53
a) Fase de preparación .....	53
b) Fase de prueba .....	53
c) Fase de conclusión .....	55
5. Consecuencias de las pruebas de penetración basadas en amenazas: el Plan corrector e Informe de validación.....	55
6. Cooperación y reconocimiento mutuo .....	56
<b>III. LA SOLUCIÓN DE LOS INCIDENTES OPERATIVOS DIGITALES .....</b>	<b>56</b>
A) La detección de los incidentes operativos digitales..	57
B) La clasificación de los incidentes operativos digitales y de las ciberamenazas.....	58
1. Incidentes relacionados con las TIC .....	58
2. Ciberamenazas.....	59
C) La notificación de los incidentes operativos digitales y de las ciberamenazas.....	59

1. La notificación obligatoria de los incidentes graves relacionados con las TIC .....	59
2. La notificación voluntaria de las ciberamenazas importantes .....	60
3. El aprovechamiento de la información por las autoridades de supervisión .....	60
<b>IV. LA GESTIÓN DEL RIESGO OPERATIVO DIGITAL DERIVADO DE TERCEROS .....</b>	<b>61</b>
A) El principio de especialización de las actividades económicas y la necesidad de las entidades financieras de externalizar o subcontratar servicios TIC con terceros proveedores.....	61
B) Regulación: los “principios fundamentales de una buena gestión del riesgo relacionado con las TIC derivado de terceros” .....	63
1. La responsabilidad .....	63
2. La proporcionalidad .....	63
C) Contratación.....	65
1. Precontractual .....	65
2. Contractual .....	66
3. Post-contractual .....	67
<b>CAPÍTULO 4</b>	
<b>CONTROL PÚBLICO,</b>	
<b>SUPERVISIÓN, SANCIÓN Y</b>	
<b>CIBERDELINCUENCIA .....</b>	<b>69</b>
<b>I. SUPERVISIÓN .....</b>	<b>69</b>
A) Supervisión privada por las propias entidades financieras o autosupervisión .....	69
B) Supervisión pública por las autoridades competentes .....	70
1. Autoridades públicas supervisoras .....	71

1.1. Las Autoridades Europeas de Supervisión .....	71
1.2. El Foro de Supervisión .....	72
1.3. El supervisor principal .....	73
2. Sujetos supervisados .....	73
3. Las Directrices conjuntas de las Autoridades Europeas de Supervisión sobre la cooperación en materia de supervisión y sobre el intercambio de información en virtud de DORA. Resolución de 17 de diciembre de 2024 de la DGSFP .....	73
II. SANCIÓN .....	77
A) La sujeción .....	77
B) La infracción.....	78
C) La sanción.....	78
III. RESPONSABILIDADES DE LAS ENTIDADES FINANCIERAS DERIVADAS DE INCIDENTES DIGITALES .....	79
A) Antecedentes jurisprudenciales sobre cibercriminalidad y fraudes informáticos en el mercado bancario.....	79
1. Sentencias de la Sala Segunda de lo Penal del Tribunal Supremo .....	79
a) La Sentencia de la Sala Segunda de lo Penal del Tribunal Supremo de 16 de febrero de 2017: El caso “MINAS DE ALMADÉN” .....	79
b) La Sentencia núm.369/2019 de la Sala de lo Penal del Tribunal Supremo de 20 de junio de 2019: El caso “BITCO-CHO” .....	82

2. La Sentencia de la Sala Primera de lo Civil del Tribunal Supremo núm. 571/2025, de 9 de abril de 2025 .....	89
3. Las Sentencias de las Audiencias Provinciales ..	97
B) El caso REDSYS como prueba de los fallos en los principales sistemas de pago bancarios y en otras plataformas de pago.....	98
1. El supuesto de hecho.....	98
2. La necesidad de implantar los mecanismos de resiliencia operativa digital de las entidades financieras previstos en DORA .....	99
C) La necesaria distinción entre las ciberestafas a los clientes bancarios usuarios en la prestación de servicios de pago y a los inversores con ánimo de especulación en el mercado de criptoactivos ..	102
D) Conclusión: el punto de equilibrio entre la doble diligencia preventiva (DDP), profesional, de los bancos y usual de los clientes .....	102
<b>CAPÍTULO 5</b>	
<b>APLICACIÓN DEL DORA EN ESPAÑA.....</b>	<b>105</b>
<b>I. DERECHO ESPAÑOL. LA LEY DE LOS MERCADOS DE VALORES Y DE LOS SERVICIOS DE INVERSIÓN ADAPTA EL RÉGIMEN DE LAS EMPRESAS DE SERVICIOS DE INVERSIÓN AL DORA.....</b>	<b>105</b>
A) La LMVSI .....	105
B) El “Informe del resultado de la autoevaluación sobre la preparación de las entidades respecto a DORA” de la CNMV de 12 de diciembre de 2024 .....	106
1. Finalidad .....	106
2. Contenido .....	107
3. Conclusiones.....	108

II. ADAPTACIÓN AL DORA DEL RÉGIMEN SANCIONADOR APLICABLE A LAS EMPRESAS DE SERVICIOS DE INVERSIÓN.....	109
A) En la tipificación de sus incumplimientos como infracciones muy graves o graves .....	110
B) En el régimen de las sanciones imponibles .....	111
III. AJUSTE TEMPORAL DE LA ADAPTACIÓN AL DORA DEL RÉGIMEN SANCIONADOR APLICABLE A LAS EMPRESAS DE SERVICIOS DE INVERSIÓN .....	113
IV. OTRAS ADAPTACIONES DE LAS SOCIEDADES GESTORAS DE IIC Y DE EIC A LA RESILIENCIA OPERATIVA DIGITAL .....	114
A) Las sociedades gestoras de IIC .....	114
B) Las sociedades gestoras de EIC .....	115
CAPÍTULO 6	
CONCLUSIONES .....	117
BIBLIOGRAFÍA .....	125

**Esta monografía** sigue la serie de las monografías sobre la Digitalización Mercantil Europea (DME) inscritas en la Colección de Derecho Mercantil de la Editorial Reus, fijando su atención en la resiliencia operativa digital del sector financiero regulada en el Reglamento (UE) 2022/2554, conocido por sus acrónimo anglosajón DORA.

Esta obra pretende servir de **guía básica que ayude a los estudiantes y profesionales** para no perderse en la jungla de conceptos y normas que pueblan el ecosistema de la resiliencia operativa digital del sector financiero y, para ello, ordena su contenido en **seis capítulos** que tratan de los aspectos generales de DORA (Capítulo 1); de su estructura, exponiendo los elementos subjetivos (entidades financieras incluidas y excluidas) y objetivos (riesgo, incidente y resiliencia) (Capítulo 2); de su funcionamiento conforme a un proceso trifásico de gestión del riesgo operativo digital, prevención del incidente operativo digital, y solución de los incidentes operativos digitales (Capítulo 3); de los instrumentos del control de la aplicación de DORA incluyendo la supervisión privada por las propias entidades financieras o autosupervisión y la supervisión pública por las autoridades competentes y la ciberdelincuencia en el ámbito financiero se (Capítulo 4); y de su adaptación en la Ley de los mercados de valores y de los servicios de inversión (Capítulo 5). Acaba ofreciendo al lector unas conclusiones que sintetizan en unas pocas páginas el contenido de esta obra (Capítulo 6).

**Alberto J. Tapia Hermida** es Catedrático de Derecho Mercantil de la Universidad Complutense de Madrid y Consejero académico de Estudio Jurídico Sánchez Calero. Está especializado en la exposición y análisis del mercado financiero en sus tres segmentos: mercado bancario, mercado de valores y mercado de seguros y fondos de pensiones. Es autor de un blog de regulación financiera (ajatapia.com) y ha dedicado gran parte de su obra reciente a la regulación de la inteligencia artificial en la UE y a la digitalización mercantil europea en general y en el sector financiero en particular.