

ÍNDICE

CAPÍTULO 1. ASPECTOS GENERALES

I. ÁMBITO DE APLICACIÓN INTERNO Y EXTERNO

A) Ámbito interno

B) Ámbito externo

II. VIGENCIA

III. CONTEXTO NORMATIVO

A) La inserción de DORA en el Paquete Europeo de Finanzas Digitales

B) La complementariedad de DORA con el sistema de gestión del riesgo de las entidades financieras basado en el capital

C) La supletoriedad del DORA

1. Genérica

2. Específica

IV. CARACTERÍSTICAS DE DORA

A) El carácter directamente vinculante de DORA

B) La proporcionalidad en la aplicación del DORA

V. CONTEXTO ECONÓMICO: LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)

CAPÍTULO 2. ESTRUCTURA DEL DORA

I. ELEMENTOS SUBJETIVOS: LAS ENTIDADES FINANCIERAS

A) Entidades financieras incluidas

1. Entidades del mercado bancario

2. Entidades del mercado de valores

3. Entidades del mercado de seguros

4. Entidades transversales a los tres sectores del mercado financiero

B) Entidades financieras excluidas

II. ELEMENTOS OBJETIVOS: RIESGO, INCIDENTE Y RESILIENCIA

A) El riesgo

B) El incidente

C) La resiliencia

CAPÍTULO 3. FUNCIONAMIENTO DEL DORA

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

B) El establecimiento de un marco de gestión del riesgo operativo digital relacionado con las TIC

1. Requisitos de calidad del marco de gestión del ROD: adecuación, fiabilidad, capacidad y resiliencia

2. Requisitos de cantidad o contenido del marco de gestión del ROD: estrategias, políticas, procedimientos, y protocolos y herramientas

C) Gobernanza y control del marco interno de gestión del ROD por el órgano de dirección de la entidad financiera

D) Ejecución del marco de gestión del ROD

1. La protección y prevención

2. La detección de actividades anómalas

3. Respuesta y recuperación

4. Aprendizaje y evolución

5. Comunicación

II. LA PREVENCIÓN DEL INCIDENTE OPERATIVO DIGITAL: LAS PRUEBAS DE RESILIENCIA OPERATIVA DIGITAL

A) Programas de pruebas

1. Requisitos objetivos de las pruebas normales y avanzadas

a) Pruebas normales

b) Pruebas avanzadas

2. Requisitos subjetivos de los probadores externos e internos

a) Probadores externos

b) Probadores internos

B) Pruebas de penetración basadas en amenazas: El Reglamento Delegado 2025/1190 de la Comisión Europea

1. Aspectos generales

2. Ámbito de aplicación: entidades financieras obligadas a realizar pruebas de penetración basadas en amenazas

a) Los criterios de selección

b) Los tipos de entidades financieras seleccionadas

3. Gestión de las pruebas de penetración basadas en amenazas

a) Las autoridades competentes: los equipos de ciberseguridad y los gestores de pruebas de penetración basadas en amenazas

b) Las entidades financieras seleccionadas: sus disposiciones organizativas

c) La gestión de riesgos de las pruebas de penetración basadas en amenazas

4. Cronología de las pruebas de penetración basadas en amenazas

a) Fase de preparación

b) Fase de prueba

c) Fase de conclusión

5. Consecuencias de las pruebas de penetración basadas en amenazas: el Plan corrector e Informe de validación

6. Cooperación y reconocimiento mutuo

III. LA SOLUCIÓN DE LOS INCIDENTES OPERATIVOS DIGITALES

A) La detección de los incidentes operativos digitales

B) La clasificación de los incidentes operativos digitales y de las ciberamenazas

1. Incidentes relacionados con las TIC

2. Ciberamenazas

C) La notificación de los incidentes operativos digitales y de las ciberamenazas

1. La notificación obligatoria de los incidentes graves relacionados con las TIC

2. La notificación voluntaria de las ciberamenazas importantes

3. El aprovechamiento de la información por las autoridades de supervisión

IV. LA GESTIÓN DEL RIESGO OPERATIVO DIGITAL DERIVADO DE TERCEROS

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

B) Regulación: los “principios fundamentales de una buena gestión del riesgo relacionado con las TIC derivado de terceros”

1. La responsabilidad

2. La proporcionalidad

C) Contratación

1. Precontractual

2. Contractual

3. Post-contractual

CAPÍTULO 4. CONTROL PÚBLICO, SUPERVISIÓN, SANCIÓN Y CIBERDELINCUENCIA

I. SUPERVISIÓN

A) Supervisión privada por las propias entidades financieras o autosupervisión

B) Supervisión pública por las autoridades competentes

1. Autoridades públicas supervisoras

1.1. Las Autoridades Europeas de Supervisión

1.2. El Foro de Supervisión

1.3. El supervisor principal

2. Sujetos supervisados

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

II. SANCIÓN

A) La sujeción

B) La infracción

C) La sanción

III. RESPONSABILIDADES DE LAS ENTIDADES FINANCIERAS DERIVADAS DE INCIDENTES DIGITALES

A) Antecedentes jurisprudenciales sobre ciberdelincuencia y fraudes informáticos en el mercado bancario

1. Sentencias de la Sala Segunda de lo Penal del Tribunal Supremo

a) La Sentencia de la Sala Segunda de lo Penal del Tribunal Supremo de 16 de febrero de 2017: El caso “MINAS DE ALMADÉN”

b) La Sentencia núm.369/2019 de la Sala de lo Penal del Tribunal Supremo de 20 de junio de 2019: El caso “BITCOCHO”

2. La Sentencia de la Sala Primera de lo Civil del Tribunal Supremo núm. 571/2025, de 9 de abril de 2025

3. Las Sentencias de las Audiencias Provinciales

B) El caso REDSYS como prueba de los fallos en los principales sistemas de pago bancarios y en otras plataformas de pago

1. El supuesto de hecho

2. La necesidad de implantar los mecanismos de resiliencia operativa digital de las entidades financieras previstos en DORA

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

D) Conclusión: el punto de equilibrio entre la doble diligencia preventiva (DDP), profesional, de los bancos y usual de los clientes

CAPÍTULO 5. APLICACIÓN DEL DORA EN ESPAÑA

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

A) La LMVSI

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

1. Finalidad

2. Contenido

3. Conclusiones

II. ADAPTACIÓN AL DORA DEL RÉGIMEN SANCIONADOR APLICABLE A LAS EMPRESAS DE SERVICIOS DE INVERSIÓN

A) En la tipificación de sus incumplimientos como infracciones muy graves o graves

B) En el régimen de las sanciones imponibles

III. AJUSTE TEMPORAL DE LA ADAPTACIÓN AL DORA DEL RÉGIMEN SANCIONADOR APLICABLE A LAS EMPRESAS DE SERVICIOS DE INVERSIÓN

IV. OTRAS ADAPTACIONES DE LAS SOCIEDADES GESTORAS DE IIC Y DE EIC A LA RESILIENCIA OPERATIVA DIGITAL

A) Las sociedades gestoras de IIC

B) Las sociedades gestoras de EIC

CAPÍTULO 6. CONCLUSIONES

BIBLIOGRAFÍA