ÍNDICE

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