CNMV
COMISIÓN NACIONAL DEL MERCADO DE VALORES

RESILIENCIA OPERATIVA EN LOS MERCADOS DE VALORES

Desarrollo de los Mercados de Valores

Colaboración con FIAB

Panamá, marzo 2026

FRANCISCO DEL OLMO
SUBDIRECTOR FINTECH & CIBERSEGURIDAD
folmo@cnmv.es
CNMV España

RESILIENCIA OPERATIVA DEL SISTEMA FINANCIERO

Resiliencia:

Capacidad de una organización para resistir, adaptarse y recuperarse eficazmente ante perturbaciones, riesgos o cambios adversos, manteniendo o restableciendo su funcionamiento esencial.

…. aplicado a los servicios TIC que soportan las operaciones del negocio

CNMV
COMISIÓN NACIONAL DEL MERCADO DE VALORES

RESILIENCIA OPERATIVA DEL SISTEMA FINANCIERO

AMENAZAS

- Vectores de ataque
- Cibercrimen y geopolítica
- Proveedores
- Tecnologías emergentes

REGULACIÓN

27.12.2022 Diario Oficial de la Unión Europea L 333/1

I

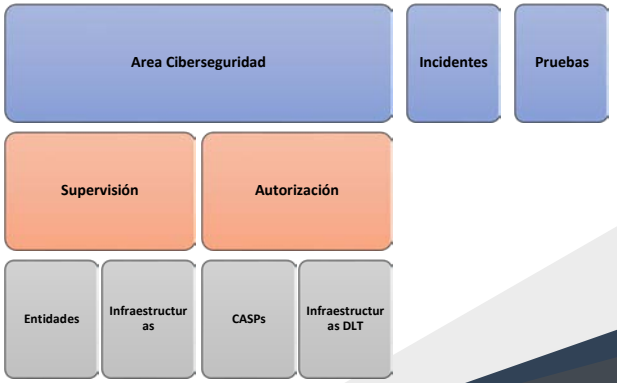
(Actos legislativos)

REGLAMENTOS

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, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011

(Texto pertinente a efectos del EEE)

CNMV



CNMV
COMISIÓN NACIONAL DEL MERCADO DE VALORES

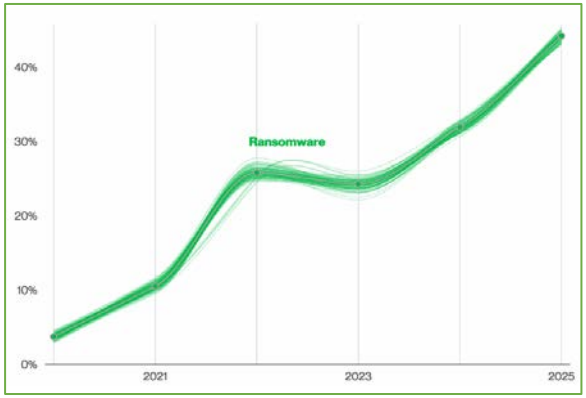
RESILIENCIA OPERATIVA DEL SISTEMA FINANCIERO

Vectores de ataque

GLOBAL

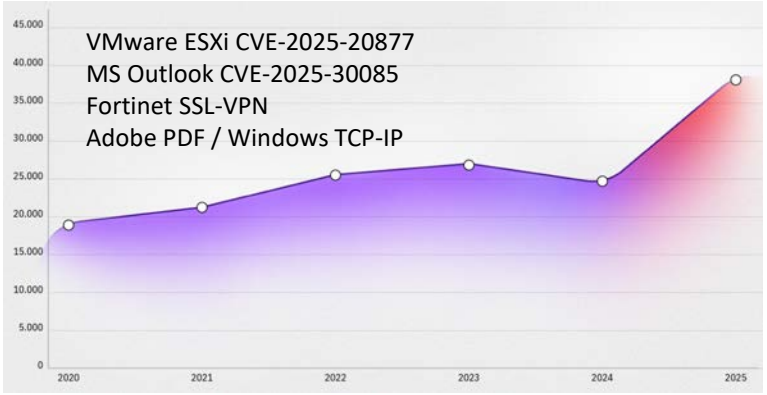
- Aumento de **phishing** y explotación de credenciales
- Explotación de **vulnerabilidades** y Zero-Day
- **Ransomware**: crecimiento y transformación
- **DDoS**: sigue siendo el incidente más numeroso.

Ransomware



Verizon: 2025 Data Breach Investigations Report

Vulnerabilidades



IBM: X-Force Threat Intelligence Index 2026

Phishing multicanal, además de correo electrónico:

- SMS (smishing)
- Llamadas (vishing)
- Mensajería instantánea
- Plataformas colaborativas

Strela Stealer

Spear-phishing

Phishing automatizado (PhaaS)

Credential harvesting

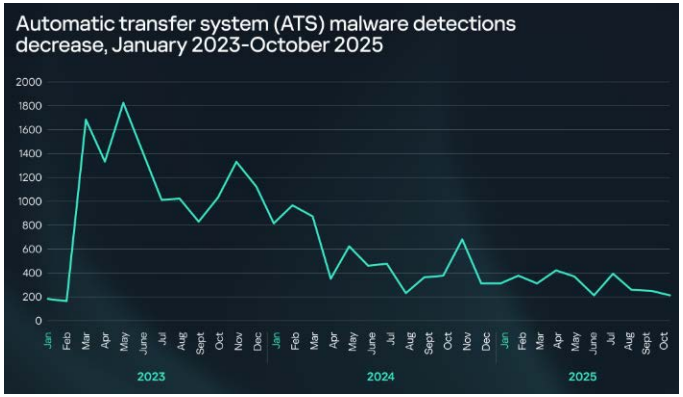
Vectores de ataque

SECTOR FINANCIERO

- **Fraude digital**: BEC, vishing y account takeover.
- **Ransomware**: foco en proveedores de servicios
- **Malware móvil**: apps y pasarelas de pago (ATS/NFC)
- **Credenciales robadas**: ataques a API
- **DDoS dirigido**: reputación y disponibilidad.

ATS

NFT



KSB: Financial sector threat landscape in 2025

APIs

Vector de ataque

- credenciales robadas
- Explotación de vulnerabilidades de diseño
- Inyección y manipulación de parámetros
- Ataques de denegación de servicio
- Exposición de terceros

Tendencias

- Incremento de ataques automatizados
- Aumento de Open Banking y Open Finance
- Ataques combinados

Mitigación

- Autenticación robusta
- Validación y filtrado de entradas
- Monitorización y alertas
- Pruebas y auditorías
- Control de proveedores

RESILIENCIA OPERATIVA DEL SISTEMA FINANCIERO

Cibercrimen

En el sector financiero europeo, los ataques DDoS representan la mayoría de incidentes.

BCE: "el contexto geopolítico actual, los ciberataques patrocinados por Estados pueden afectar a la estabilidad financiera si impactan a entidades o infraestructuras críticas sin sustitutos inmediatos. El el sector financiero el riesgo se incrementa por su alta interconexión entre las entidades y con otros sectores, que amplifica el impacto".

CONFLICTO ARMADO ENTRE RUSIA Y UCRANIA

Ciberespionaje y Ciberataques

Hacktivistas

Desinformación e Influencia Estratégica

- **17%** de las brechas analizadas en 2025 tenían motivación de **espionaje** (state-sponsored)
- **28%** de incidentes de actores estatales tenían un motivo **financiero** además del espionaje

Verizon. 2025 Data Breach Investigations Report

China, Rusia, Irán y Corea del Norte son los actores estatales más activos, usando ciberataques para:

- Espionaje económico y financiero
- Sabotaje de infraestructuras críticas
- Robos de datos, cripto, BEC y ransomware para financiar operaciones

Top Threat Actors

	2021	2022	2023	2024	2025
#1 Threat Actor	Malicious insiders	Human error	Human error	External attackers — hacktivists	External attackers — hacktivists
#2 Threat Actor	Human error	External attackers — hacktivists	External attackers — hacktivists	Human error	External attackers — nation-state actors
#3 Threat Actor	External attackers	External attackers — nation-state actors	External attackers — nation-state actors	External attackers — nation-state actors	Human error

CNMV
COMISIÓN NACIONAL DEL MERCADO DE VALORES

RESILIENCIA OPERATIVA DEL SISTEMA FINANCIERO

Cadena de proveedores

El sector financiero es especialmente vulnerable porque muchas instituciones **dependen** de los mismos proveedores tecnológicos. Pudiendo tener efectos **sistémicos** sobre la estabilidad financiera.

¿QUÉ HACER?

- **Due dilligence** previa
- identificar **proveedores críticos** y gestión del riesgo
- mapear **dependencias y concentraciones** tecnológicas
- evaluar riesgos derivados de **dependencia excesiva de un único proveedor o infraestructura**
- **Contrato de nivel de servicio**
- Estrategia de **salida**

AMENAZAS

- Explotación de **vulnerabilidades** en software utilizado por muchas organizaciones
- Falta de visibilidad sobre el **nivel real de seguridad** de terceros
- **Persistencia** dentro de entornos comprometidos para mantener acceso prolongado.
- **Librerías** open-source manipuladas
- Servicios cloud o plataformas **compartidas**

AMPLIFICA RIESGOS

- **Externalización creciente de servicios tecnológicos**
- Dependencia de **cloud providers y SaaS**
- Uso masivo de **software open-source**
- **Concentración de proveedores** en sectores críticos
- Complejidad del ecosistema de **subcontratación multinivel**
- Falta de **monitorización continua de proveedores**

CONSECUENCIAS

- **Interrupción** de servicios críticos
- Impactos **financieros** y compensaciones a clientes
- **Sanciones** regulatorias
- Impactos **reputacionales** y pérdida de confianza
- exposición pública de **datos**.

CNMV
COMISIÓN NACIONAL DEL MERCADO DE VALORES

RESILIENCIA OPERATIVA DEL SISTEMA FINANCIERO

USO DE LA IA EN CIBERATAQUES

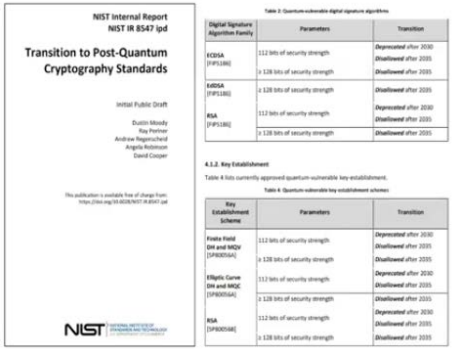
- Phishing y campañas de **ingeniería social**
- IA para explotación de **vulnerabilidades**
- **Manipulación** de información y desinformación
- Falsificación de **identidad**
- **Automatizar ataques** en entornos críticos

Tecnologías emergentes

- Inteligencia artificial
- Cuantum Computing

Pero también:

- Riesgo en su uso sin un **gobierno de IA** adecuado
- En herramientas de **detección** de ciberataques


NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8547.ipd

NIST

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	Disallowed after 2035
RSA [FIPS186]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035

4.1.2. Key Establishment

Table 4 lists currently approved quantum-vulnerable key establishment.

Table 4: Quantum-vulnerable key establishment schemes

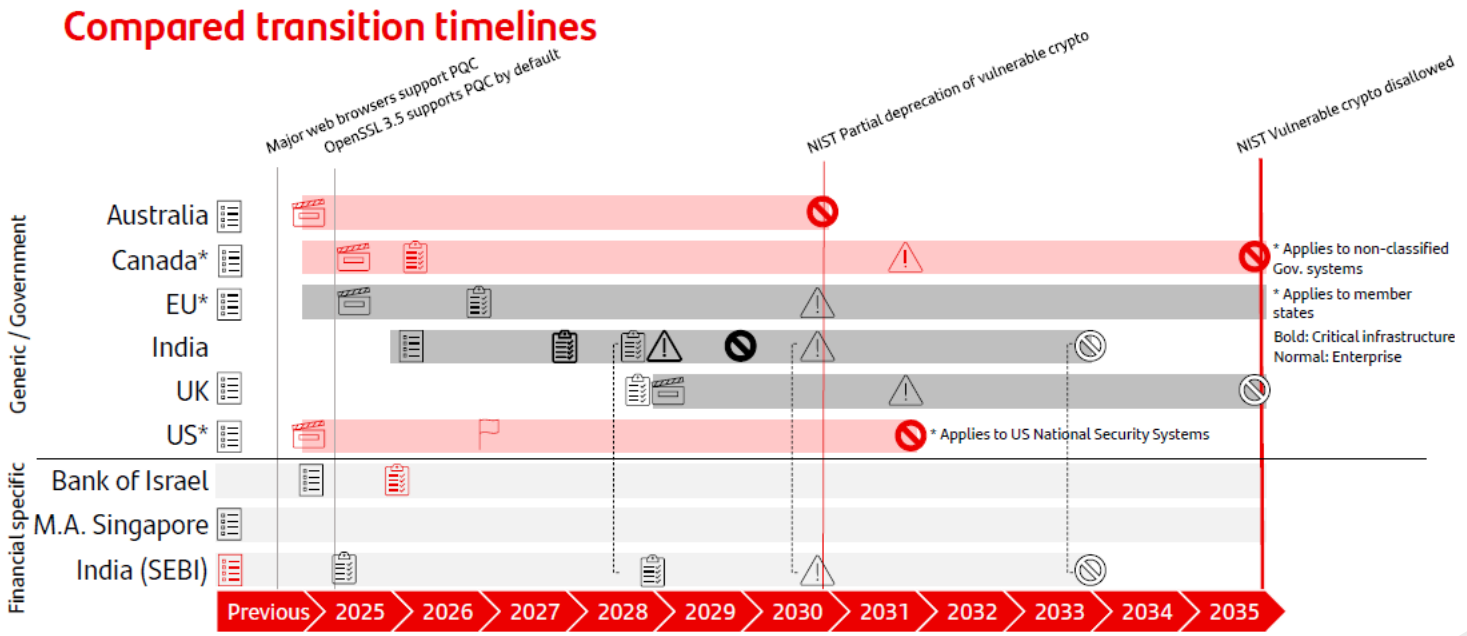
Key Establishment Scheme	Parameters	Transition
Finite Field DH and MQV [SP80056A]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035
Elliptic Curve DH and MQV [SP80056A]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035
RSA [SP80056B]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035

QUANTUM COMPUTING

- **Romper algoritmos criptográficos clásicos**, especialmente aquellos basados en factorización de enteros (RSA) y logaritmos discretos (ECC)
- "**store-now, decrypt-later**"
- Se **subestima** el impacto, no se entiende la complejidad de la migración y se difiere la amenaza como un riesgo futuro probable
- Interconexión y coordinación: **todos a la vez**, sector financiero liderando
- Enorme impacto en las **infraestructuras** de mercado y sistemas de pago

RESILIENCIA OPERATIVA DEL SISTEMA FINANCIERO

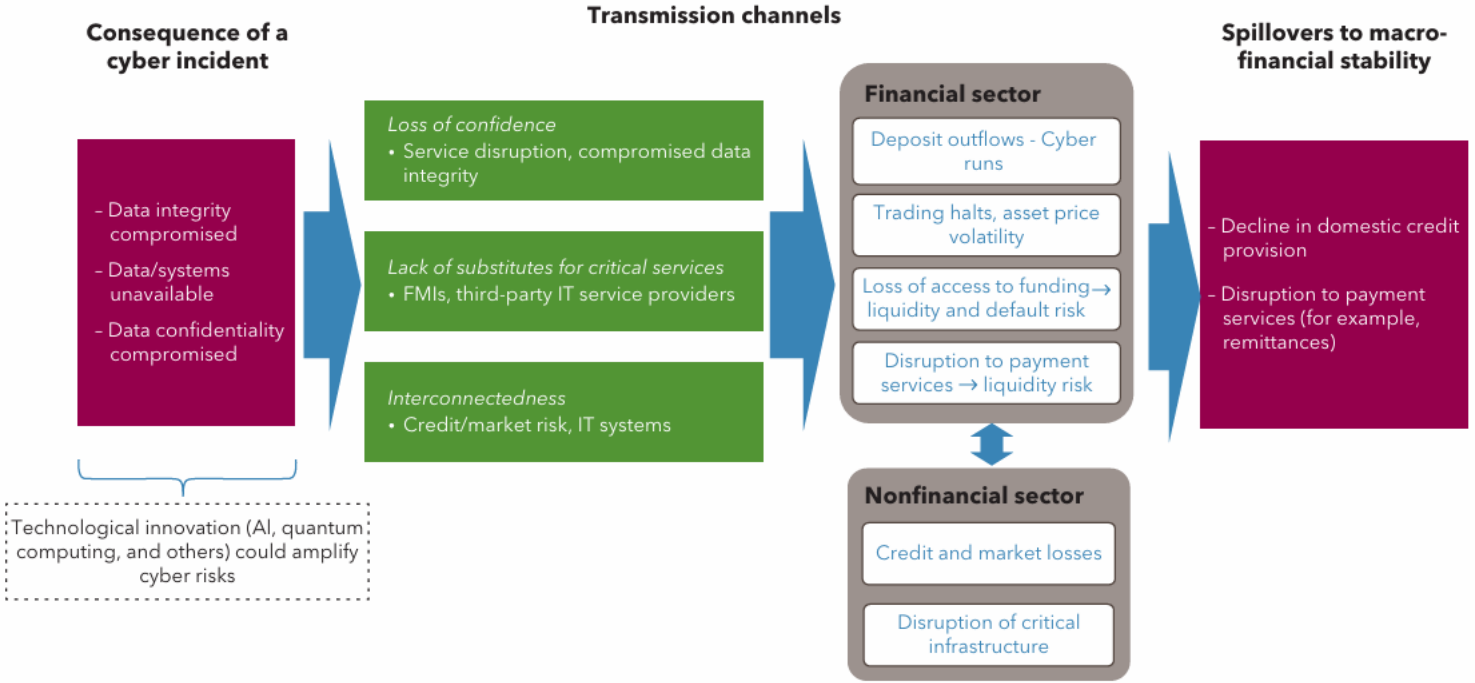
QUANTUM SAFETY



Jaime Gómez García- Banco Santander

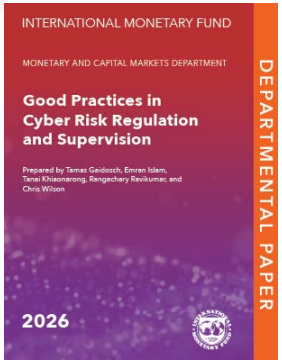
RESILIENCIA OPERATIVA DEL SISTEMA FINANCIERO

Impacto en las infraestructuras de mercado



Source: IMF 2024c.

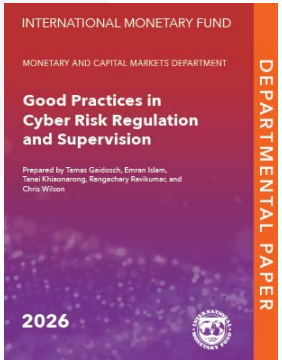
Note: AI = artificial intelligence; FMIs = financial market infrastructures; IT = information technology.



CNMV
COMISIÓN NACIONAL DEL MERCADO DE VALORES

RESILIENCIA OPERATIVA DEL SISTEMA FINANCIERO

Regulación y supervisión



BUENAS PRÁCTICAS REGULATORIAS

- Regulación unificada: integrar TIC + riesgo cibernético.
- Enfoque principios + prescriptivo, adaptado a la madurez de la institución.
- Proporcionalidad según tamaño, complejidad y criticidad.
- Gobernanza sólida, auditorías internas y externas.
- Pruebas de vulnerabilidad y planes de continuidad del negocio.

BUENAS PRÁCTICAS DE SUPERVISIÓN

Modalidades:

- Off-site: monitoreo continuo de métricas y reportes cibernéticos, mapeo de riesgos.
- On-site: revisión directa de infraestructura, entrevistas, pruebas y validación de controles.
- Revisiones temáticas: estudios horizontales de riesgos o áreas específicas.

Elementos clave:

- Personal capacitado (CISA, CISSP, especialistas técnicos).
- Integración de ciberresiliencia en la supervisión general.
- Participación de la junta y modelado de riesgo de terceros.

EJERCICIOS DE SIMULACIÓN

Objetivo: Probar respuesta, coordinación y recuperación ante incidentes.

Tipos de ejercicios:

- Phishing y concienciación.
- Tabletop / walkthrough (planes de respuesta).
- Threat-led penetration testing (TLPT), red/blue team.
- Crisis management a nivel ejecutivo y sectorial.

Beneficios:

- Identificación de vulnerabilidades.
- Mejora de comunicación y coordinación.
- Cumplimiento regulatorio.
- Preparación frente a nuevas amenazas.
- Buenas prácticas: compromiso de stakeholders, planificación multianual, evaluación y mejora continua.

SEGUIMIENTO RIESGO SISTÉMICO

- Identificación de terceros críticos y dependencias tecnológicas.
- Evaluación de concentraciones de riesgo y puntos únicos de fallo.
- Estrategias:
  - Supervisión continua.
  - Reporte y análisis de incidentes.
  - Mapas de interdependencias.
  - Pruebas de estrés y métricas de resiliencia.
  - FMIs requieren supervisión + oversight robusto por su impacto sistémico

CNMV
COMISIÓN NACIONAL DEL MERCADO DE VALORES

RESILIENCIA OPERATIVA DEL SISTEMA FINANCIERO

Reglamento DORA

Reglamento DORA	NIST	ISO 27000
Ley	Guías	Estandar
Obligatorio Ent. Financieras	Recomendaciones	Certificado

	Ámbitos DORA	Capítulo	Descripción
	**Gestión de Riesgos TIC**	**II**	• Gobernanza y organización. • Marco de gestión de riesgo TIC. • Identificación, protección y prevención, detección, respuesta y recuperación, aprendizaje y evolución, y comunicación. • Continuidad de la actividad
	**Gestión de Incidentes TIC**	**III**	• Gestión, clasificación y notificación de incidentes. • Obligaciones de información a todas las entidades financieras.
	**Pruebas de la Resiliencia Operativa**	**IV**	• Realización de pruebas básicas o avanzadas por parte de las entidades financieras.
	**Gestión de Riesgos de Terceros**	**V**	• Normas y principios para supervisar el riesgo de terceros. • Disposiciones contractuales clave. • Marco de supervisión para los proveedores TIC esenciales.

RESILIENCIA OPERATIVA DEL SISTEMA FINANCIERO

Reglamento DORA

Proporcionalidad

Las entidades financieras **aplicarán las normas** establecidas 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.**

Marco simplificado de gestión de riesgos TIC

ESI pequeña no interconectada

Exenciones para

Microempresas: Entidad financiera distinta de un centro de negociación, una entidad de contrapartida central, un registro de operaciones o un depositario central de valores, que emplea a **menos de diez personas** y cuyo volumen de negocios anual o balance anual total es igual o inferior a **2 millones €.**

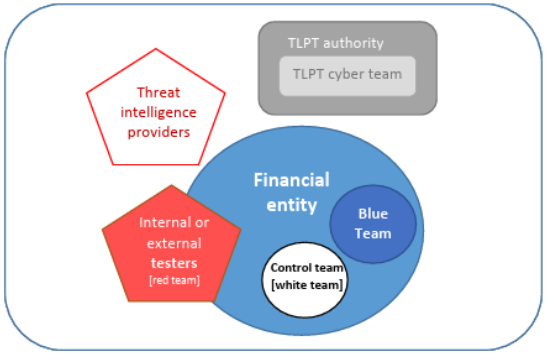
Exigencias adicionales

Infraestructuras de Mercado: Exigencias concretas en el ámbito de las pruebas de continuidad de negocio, planes de recuperación, centros de proceso secundarios y gestión de vulnerabilidades.

El marco TIBER-ES de pruebas avanzadas

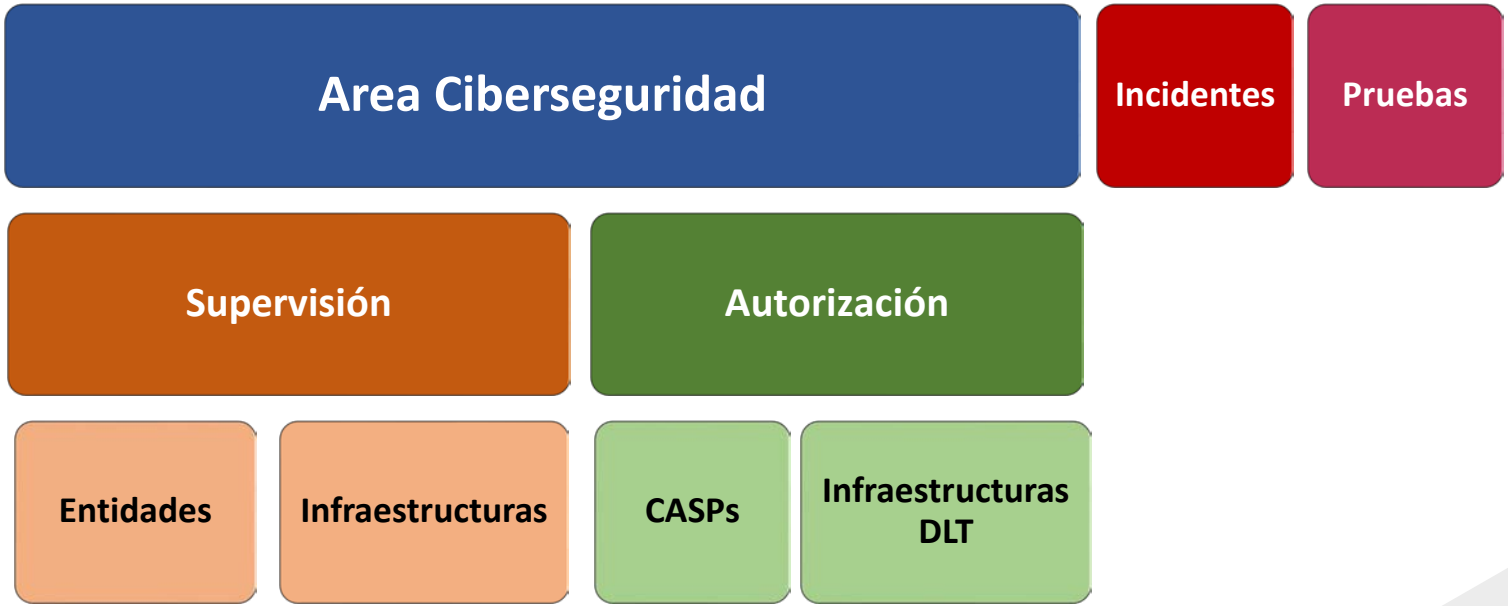
- Marcos **TIBER-EU** (ECB) / Pruebas TLPT: artículos 26 y 27 de DORA y RTS.
- **TIBER-ES** (BdE, CNMV y Seguros).
- Simular un ciberataque empleando tácticas, técnicas y procedimientos como los que utilizaría un ciberatacante **sofisticado**, sin el conocimiento de la mayor parte de empleados de la entidad.
- **Banderas** objetivo sobre funciones críticas en entornos de producción.
- **Fases**: preparación, test y cierre.
- **Roles y responsabilidades**:

  - Entidad:
    White Team: equipo de control
    Blue Team: equipo defensivo
  - Proveedor:
    Equipo de inteligencia: recopilación previa
    Red Team: equipo ofensivo
  - TCT: autoridad supervisora



Hallazgos relevantes procesos supervisión

CNMV



Hallazgos relevantes procesos supervisión

Gobernanza y Organización

- Reforzar compromiso Consejo Administración. Funciones y responsabilidades no exclusivas de áreas TIC. **Se pueden delegar funciones, pero no responsabilidades**
- Carencias estructuras gobierno, separación funciones que eviten conflictos de interés. **Implantación Modelo de tres líneas de defensa**
- **Establecer canales para reporte y seguimiento del Consejo Administración** de riesgos TIC, especialmente **ante hallazgos significativos o graves**
- Revisar y reforzar asignación presupuestaria destinada a resiliencia operativa digital. **Se detecta una baja dotación de partidas para adecuación a DORA.**
- **Falta programas formación en riesgos TIC dirigidos al Consejo de Administración**

Hallazgos relevantes procesos supervisión

Marco de gestión de riesgos TIC

- **Carencias estrategias resiliencia, adolecen aspectos: nivel de tolerancia al riesgo, medidas y controles, planes** de pruebas y comunicación, gestión riesgo terceros
- **Políticas y procedimientos elaborados de forma general, sin una implantación operativa real** y en algunos casos **sin ser conocidas por integrantes entidad**
- **Existen definidas medidas y controles** para la protección de los activos TIC, pero **sin un enfoque basado en riesgos**
- **Gestión riesgos TIC sin enfoque metodológico y uso herramientas adecuadas** que limitan visión global y realizar un control adecuado y continuado
- **Carencias o falta planes auditorías periódicos de riesgos TIC y seguimiento** de hallazgos graves detectados y control del Consejo de Administración

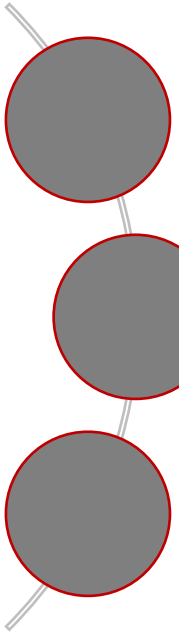
Hallazgos relevantes procesos supervisión

Continuidad de la actividad

- **BCP definidos sin perspectiva de riesgo**, sin realizar análisis de impacto (BIA) y/o sin establecer RTO y RPO para funciones esenciales o falta identificación de éstas
- **Falta pruebas de BCP, incompletas o no periódicas** para garantizar correcto funcionamiento en caso de necesidad de activación
- **Carencias o falta auditorías revisión y seguimiento formalizado deficiencias detectadas en las pruebas** del BCP y reporte al Consejo Administración

Hallazgos relevantes procesos supervisión

Aprendizaje y Evolución



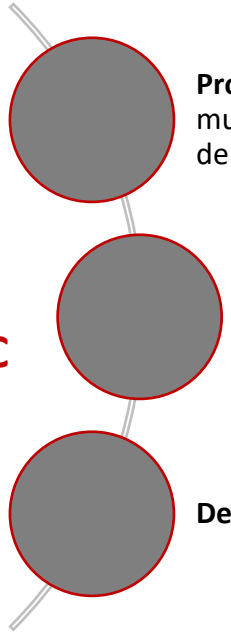
Limitación de recursos o carencias de capacitación técnica de los equipos TIC en ciberseguridad o complementadas con servicios externos especializados

Programas sensibilización y formación en seguridad TIC de alcance muy limitado y realizados puntualmente, sin seguimiento de la mejora aportada

Lecciones aprendidas de pruebas, activaciones BCP y/o incidentes TIC **no se integran en proceso gestión de riesgos TIC**, para analizar evolución del riesgo y la efectividad medidas existentes

Hallazgos relevantes procesos supervisión

Gestión de incidentes TIC



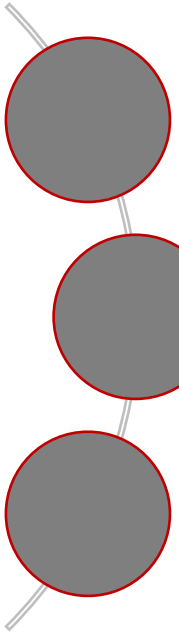
Procedimientos detección, evaluación y respuesta incidentes TIC, muy limitados, muchos basados sólo en detección por parte de usuarios, no incorporando mecanismos de detección, evaluación y respuesta automatizados

Carencias en registro y seguimiento de incidentes TIC o análisis de lecciones aprendidas para mitigar o reducir nuevas ocurrencias

Deficiencias en clasificación y notificación de incidentes TIC graves

Hallazgos relevantes procesos supervisión

Pruebas de resiliencia operativa digital



Planes o programas de pruebas sin enfoque basado en riesgos TIC o falta de seguimiento detallado del resultado de estas

Alcance muy limitado o superficial, realizándose puntualmente o sin incluir pruebas exhaustivas de detección de vulnerabilidades o test de penetración

No realizadas por probadores externos o internos independientes o no son auditadas o supervisadas por áreas distintas al área que realiza las pruebas, evitando conflictos de interés

Hallazgos relevantes procesos supervisión

Gestión del riesgo derivado de proveedores terceros TIC

- **Procedimientos evaluación muy limitados o inexistentes**
- **No se contemplan estrategias salida** proveedores soportan funciones esenciales
- Estos riesgos **no se integran dentro marco general de riesgos**
- **Falta asignación cargo** o miembro Consejo función y **responsabilidad de gestión y seguimiento riesgos y acuerdos contractuales**
- **Generalmente en proceso adecuación del clausulado** de acuerdos existentes
- **Carencias formalización acuerdos intragrupo** en entidades que pertenecen a grupos empresariales y servicios TIC prestados por la matriz
- **Dificultades en elaboración registro proveedores terceros TIC** para el reporte

RESILIENCIA OPERATIVA DEL SISTEMA FINANCIERO

1. Los **órganos de administración** de las empresas:
   - ¿tienen conocimiento e información de los los riesgos tecnológicos?
   - ¿asumen esta responsabilidad?
   - ¿gasto o inversión?
2. ¿Están preparadas las infraestructuras de mercado para activar **planes de recuperación y continuidad de negocio**?
3. ¿Se realizan **pruebas avanzadas** por terceros (Inteligencia & RT)? ¿el supervisor las monitoriza?
4. ¿Estamos preparándonos para los riesgos de las **nuevas tecnologías**?
   - Inteligencia Artificial (Generativa)
   - Quantum Safety

GRACIAS

CNMV
COMISIÓN
NACIONAL
DEL MERCADO
DE VALORES

09 / 01 / 2020