

# LA ESTRATEGIA DE CIBERRESILIENCIA DEL EUROSISTEMA PARA LAS INFRAESTRUCTURAS DE MERCADO

Miguel Pérez  
Unidad de Vigilancia y Análisis de Infraestructuras de Mercado

AMI-SeCo ESPAÑA  
16 de Noviembre de 2018



**Aprobación en marzo de 2017.**

**Objetivo:**

Establecer un **enfoque común** para hacer frente a los riesgos cibernéticos e implementar la guía de CPMI-IOSCO en el Eurosistema.

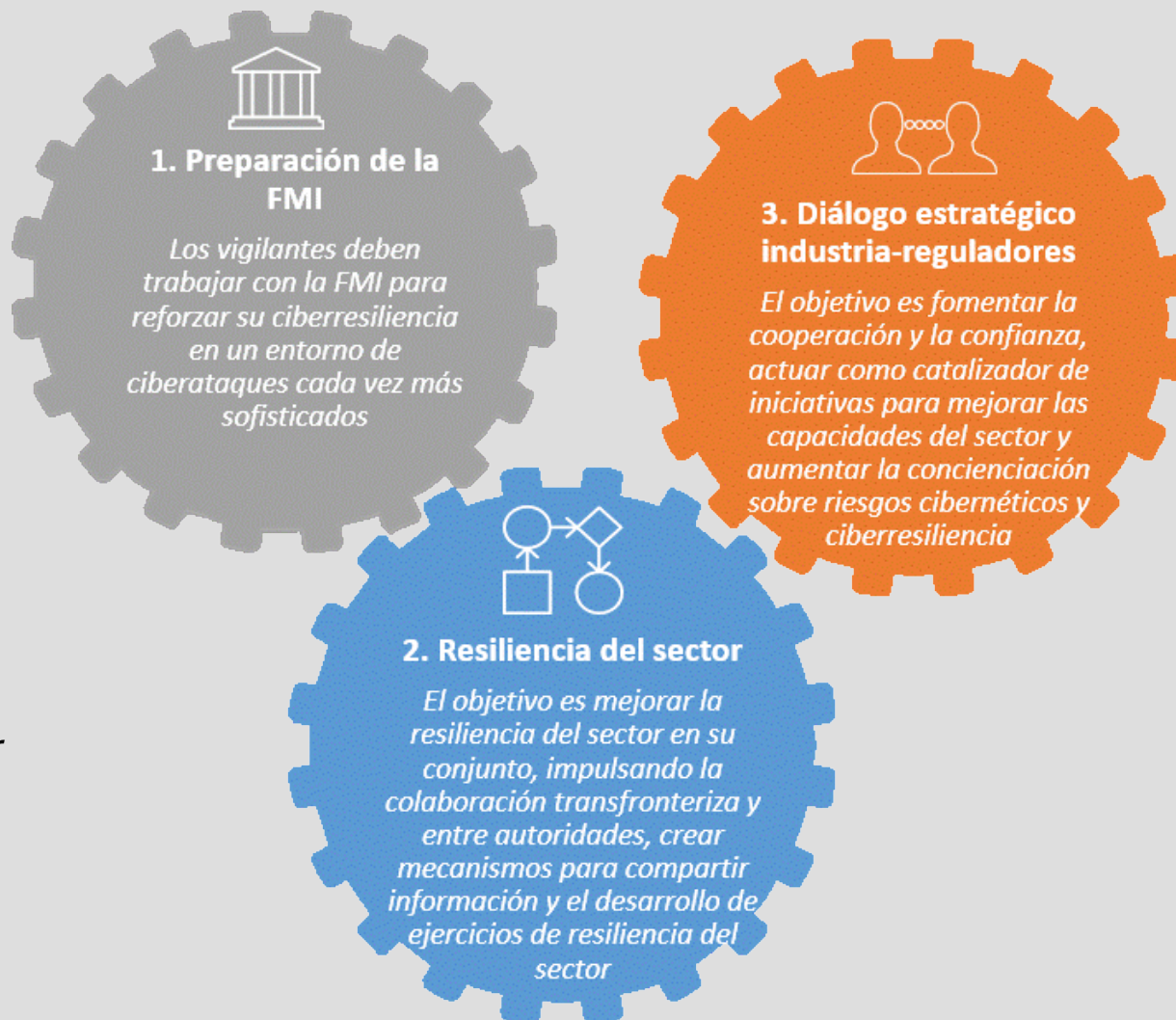
**Alcance:**

- Aquéllas FMIs que se encuentran bajo la **competencia del Eurosistema**: sistemas de pago, esquemas de tarjetas e instrumentos de pago
- No aplica a DCVs y ECCs, pero por sus interdependencias con T2 y T2S, se recomienda colaborar en el ámbito de la ciberresiliencia.
- Participación voluntaria de los **países no euro**. Participación activa en la práctica.



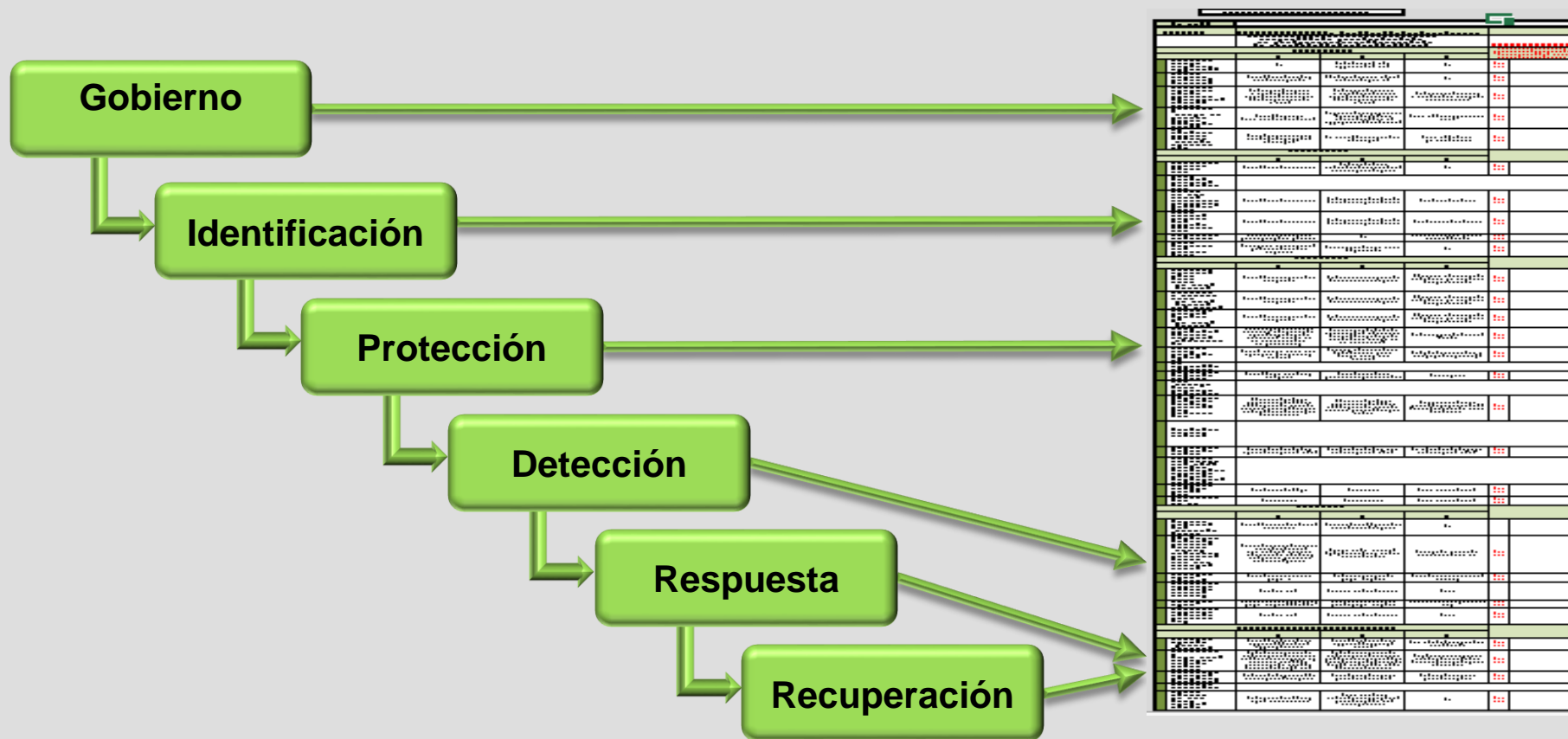
### Objetivo general:

*“En un contexto de amenazas cibernéticas cada vez mayores y fuertes interdependencias, se busca aumentar la ciberresiliencia del Eurosistema reforzando tanto la preparación de las FMIs ante estos incidentes y la del sector en su conjunto, como la colaboración.”*





## Pilar I: Contenido del cuestionario: 32 preguntas – estructura guía CPMI-IOSCO





## Pilar I: Las expectativas de vigilancia (CROE)

### Objetivos:

- Para el vigilante: las expectativas del vigilante, frente a las cuales evalúa a su FMI
- Para la FMI: Puede utilizarse para implantar la guía
- Para ambos: base para la colaboración

### Metodología:

- Recoge estándares y buenas prácticas existentes en el mercado
- Modelo de madurez en la definición de las expectativas: mejora continua
- Principio de proporcionalidad
- Principio de “comply or explain”



### Pilar I. Marco TIBER-EU de pruebas de red team

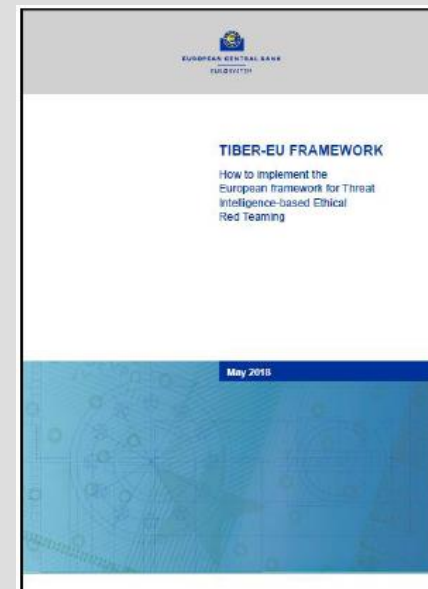
#### Threat Intelligence-based Ethical Red Teaming

#### Objetivos:

- Guía para las autoridades.
- Estandarización en la forma de realizar la pruebas.
- Marco común para el reconocimiento de los resultados.

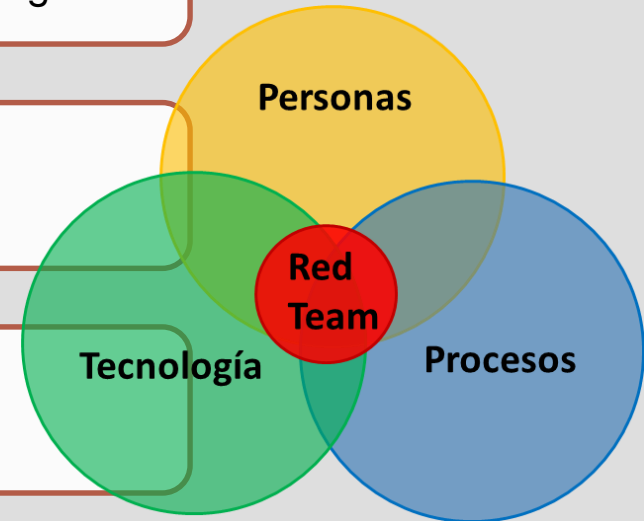
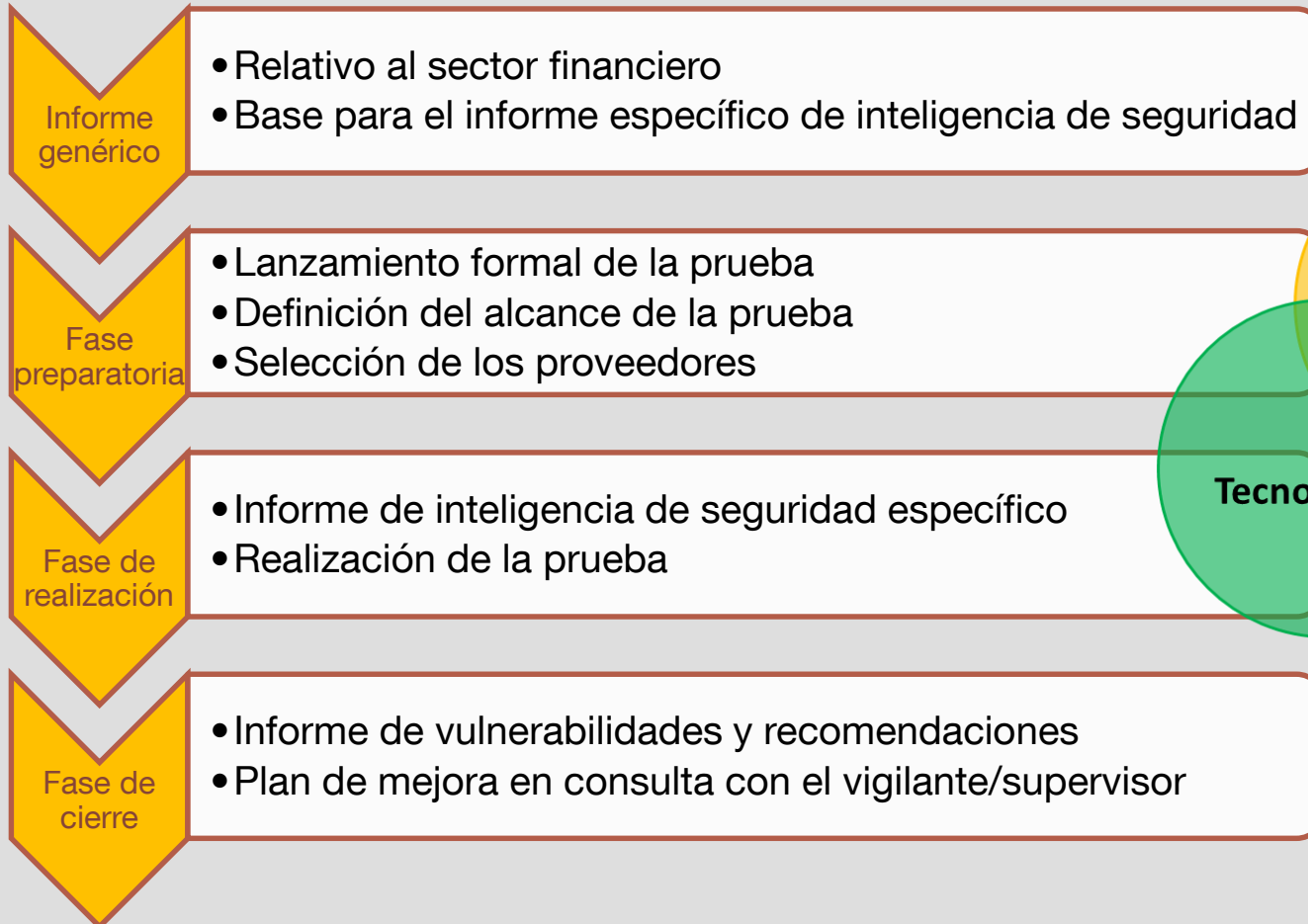
#### Principales características del marco:

- Adopción nacional.
- Creación del “*TIBER-EU Knowledge Centre*”.
- Realización por proveedores externos.



*Marco TIBER-EU aprobado por el Consejo de Gobierno en abril de 2018.*

## Fases:





## Pilar II. Resiliencia del sector

Pilar II – Resiliencia

Análisis de Nodos

Marcos de cooperación con otras autoridades:  
ENISA, ESMA, SSM

Ejercicios de simulación



UNITAS





## Pilar III – Dialogo estratégico industria reguladores

### Creación del “Euro Cyber Resilience Board for Pan-European Financial Infrastructures (ECRB)” (enero 2018)

#### Objetivos:

- Fomentar la confianza y colaboración entre las infraestructuras de mercado y los proveedores de servicios críticos y las autoridades encargadas de la vigilancia de las mismas.
- Impulsar proyectos para la concienciación sobre riesgos cibernéticos y mejorar la ciber resiliencia del sector en su conjunto identificando los temas estratégicos, estableciendo políticas y recomendaciones comunes.



GRACIAS POR SU ATENCIÓN

BANCO DE **ESPAÑA**  
Eurosistema

DEPARTAMENTO DE SISTEMAS DE PAGO



<https://www.ecb.europa.eu/paym/initiatives/cyber-resilience/html/index.en.html>

[https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber\\_eu\\_framework.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf)

<https://www.ecb.europa.eu/paym/groups/euro-cyber-board/html/index.en.html>

[https://www.ecb.europa.eu/paym/cons/html/cyber\\_resilience\\_oversight\\_expectations.en.html](https://www.ecb.europa.eu/paym/cons/html/cyber_resilience_oversight_expectations.en.html)