GUÍA DE IMPLEMENTACIÓN TIBER-ES
Threat Intelligence Based Ethical Red-Teaming - España

BANCO DE ESPAÑA
Eurosistema

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE ECONOMÍA Y APOYO A LA EMPRESA
DIRECCIÓN GENERAL DE SEGUROS Y FONDOS DE PENSIONES

CNMV
Comisión Nacional del Mercado de Valores

GUÍA DE IMPLEMENTACIÓN TIBER-ES
Threat Intelligence Based Ethical Red-Teaming - España

Enero, 2022

Índice

Abreviaturas

BT	*Blue Team*
BTTR	*Blue Team Test Report*
GTL	*Generic Threat Landscape*
RT	*Red Team*
RTTR	*Red Team Test Report*
TCT	*TIBER Cyber Team*
TI	*Threat Intelligence*
TKC	*TIBER-EU Knowledge Centre*
TLPT	*Threat Led Penetration Testing*
TTI	*Targeted Threat Intelligence*
TTM	*Team Test Manager*
TTP	*Tactics, Techniques and Procedures*
WT	*White Team*
WTL	*White Team Lead*

1 Introducción

La tecnología es un elemento imprescindible para que las entidades financieras[1] puedan ofrecer sus servicios de modo fiable, seguro y acorde con su modelo de negocio y estrategia. Factores como el elevado grado de interconexión dentro del sector financiero y con terceras partes, la continua y veloz evolución tecnológica, el aumento del número y de la sofisticación de las ciberamenazas, la digitalización de la operativa financiera o el trabajo en remoto han convertido la ciberresiliencia y la ciberseguridad de las entidades en una prioridad, desde el punto de vista tanto prudencial como de estabilidad financiera.

En este contexto, los puntos más vulnerables de las entidades pueden resultar objeto de ataques, en ocasiones altamente complejos. Por tanto, resulta fundamental que las entidades financieras reduzcan sus vulnerabilidades y dispongan de un entorno de control de la ciberseguridad efectivo y maduro. El éxito en dicha tarea, no obstante, solo será completo en la medida en que sean capaces de enfrentarse a un ciberataque real.

En ese sentido, las pruebas de *Threat Led Penetration Testing* (TLPT) o *red teaming* tienen como objetivo anticipar, en la medida de lo posible, el impacto que una entidad sufriría en caso de enfrentarse a un ciberataque real. Para ello, en este tipo de pruebas avanzadas de ciberseguridad se simula un ciberataque empleando tácticas, técnicas y procedimientos *[Tactics, Techniques and Procedures* (TTP)] como los que utilizaría un ciberatacante sofisticado. Constituyen, por tanto, un instrumento muy poderoso para mejorar la ciberresiliencia de las entidades financieras.

1 A los efectos de la presente guía, el término «entidad» se refiere no solo a cualquier entidad, institución u organización que facilita servicios financieros a clientes o miembros, sino también a las infraestructuras de mercado necesarias para la prestación de dichos servicios. En este sentido, y por simplicidad, se usará el término «entidad» para aludir indistintamente a entidad, institución, organización o infraestructura financiera.

1.1 Antecedentes

En 2016, el Banco de Inglaterra publicó el primer marco para la realización de pruebas de *red teaming* dentro del sector financiero, CBEST[2]. En la misma dirección, en 2017 los Países Bajos publicaron el marco TIBER-NL[3] *(Threat Intelligence Based Ethical Red-teaming)*, inspirado en CBEST pero con características propias. Asimismo, diferentes jurisdicciones manifestaron su intención de desarrollar marcos locales para pruebas de *red teaming.*

Ante esta situación, con el fin de evitar la fragmentación, alcanzar un grado de homogeneidad y criterios comunes en la realización de estas pruebas en Europa y evitar a las entidades financieras que operan en múltiples jurisdicciones la utilización de marcos no compatibles o la duplicidad de esfuerzos, el Banco Central Europeo (BCE) publicó, en mayo de 2018, su propio marco de pruebas avanzadas de ciberseguridad, llamado «TIBER-EU». Cualquier jurisdicción puede adoptar TIBER-EU y desarrollar su propia guía de implementación basada en el marco.

1.2 ¿Qué es TIBER-EU?

TIBER-EU constituye el primer marco común a escala europea para la realización de pruebas de *red teaming.* Este recoge el modo en que las autoridades, las entidades y los proveedores de servicios de ciberseguridad deben trabajar juntos para alcanzar el objetivo de las pruebas de *red teaming:* que la entidad que se somete a ellas detecte áreas de mejora en sus capacidades de ciberresiliencia no solo en el ámbito técnico, sino también en el personal y en el procedimental[4].

Si bien fue inicialmente concebido para entidades e infraestructuras financieras, TIBER-EU puede ser adoptado para su aplicación en cualquier tipo de entidad de cualquier sector.

El marco está diseñado para su adopción por una autoridad propietaria, cuya misión es monitorizar la realización de las pruebas y validar que se llevan a cabo de acuerdo con los requisitos del marco. El cumplimiento de los requisitos de carácter obligatorio definidos en TIBER-EU posibilita el reconocimiento mutuo de la validez de las pruebas entre las autoridades propietarias que hayan adoptado localmente el marco.

El objetivo del marco no es calificar como aprobada o suspensa a la entidad que se somete a las pruebas, sino mejorar el conocimiento de sus debilidades y fortalezas ante ciberataques e identificar medidas que incrementen su ciberresiliencia.

La realización de una prueba de *red teaming* de acuerdo con el marco TIBER-EU implica riesgos, dado que debe llevarse a cabo en entornos de producción[5]. Asimismo, el marco exige que estas

2 https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.

3 https://www.dnb.nl/media/1mdf3lmq/tiber-nl-guide.pdf.

4 Se simula un ciberataque avanzado sobre la entidad. Solo un grupo muy reducido de personas deben saber que se trata de una prueba, de modo que se puedan valorar las capacidades de protección, detección y respuesta de la entidad ante un ciberataque que cree real.

5 El entorno de producción es el conjunto de sistemas informáticos en los que se ejecutan las aplicaciones que prestan servicio a los usuarios finales, sean estos empleados de la entidad o clientes y/o donde los procesos utilizan y generan datos e información reales.

pruebas las realicen proveedores externos, con el objetivo de garantizar que las condiciones de un ciberataque se simulan del modo más realista posible, por lo que el coste de estas es elevado. Es importante señalar que los costes y los riesgos asociados a la realización de las pruebas son asumidos siempre por las entidades que se someten al test, y en ningún caso por la autoridad que adopta el marco.

Una de las características distintivas de los test TIBER-EU, en comparación con otro tipo de pruebas de ciberseguridad, es su enfoque holístico y basado en ciberinteligencia. De este modo, las entidades pueden comprobar su grado de ciberresiliencia respecto a debilidades y amenazas constatadas, relevantes para el sector y reales, en lugar de basarse solo en aquellas que la entidad percibe como tales o que es capaz de identificar usando sus propios medios.

1.3 ¿Qué es TIBER-ES?

La Comisión Ejecutiva del Banco de España aprobó, en diciembre de 2020, la adopción del marco TIBER-EU, constituyéndose en autoridad propietaria del marco nacional, si bien contará con la participación de la Comisión Nacional del Mercado de Valores (CNMV) y la Dirección General de Seguros y Fondos de Pensiones (DGSFP) cuando las entidades que vayan a someterse a las pruebas pertenezcan a sus respectivos ámbitos de competencia.

El marco nacional se denominará «TIBER-ES» y tiene como objetivo fundamental fortalecer la ciberresiliencia de las entidades financieras que operan en España. El marco se adopta desde una perspectiva de estabilidad financiera; es voluntaria la participación de las entidades en las pruebas, de modo que se les ofrece que las realicen, pero no se les exige (véase el epígrafe 1.6, «¿Quién puede someterse a este tipo de test?»).

TIBER-ES suscribe y se adhiere a los principios de TIBER-EU, de manera que las pruebas realizadas bajo el primero garantizan el reconocimiento de las autoridades en otras jurisdicciones que también han adoptado localmente el marco TIBER-EU. Para ello, se observan, entre otros, los requisitos de realizar las pruebas sobre entornos de producción y de contar con proveedores externos para la realización del test (su papel se describe en detalle en el epígrafe 2, «Participantes y funciones»). Asimismo, los costes y los riesgos asociados al proceso son asumidos íntegramente por las entidades que se someten al test.

TIBER-ES ha sido diseñado para su aplicación en la totalidad del sector financiero.

1.4 Propósito de esta guía

La presente guía de implementación forma parte del marco operativo TIBER-ES y ha sido desarrollada por el *TIBER Cyber Team* (TCT) liderado por Banco de España, en estrecha colaboración con la CNMV y la DGSFP.

El propósito del documento es especificar las condiciones para la realización de pruebas de *red teaming* bajo el esquema de requisitos de TIBER-ES. Aquellos conceptos que se consideran fundamentales y principios básicos del marco TIBER-EU han sido recogidos en el presente

documento con detalle, y las pruebas deberán ajustarse a ellos. Al margen de dichos requisitos, el documento pretende ser una guía, y no un catálogo prescriptivo de actividades.

Este documento debe ser leído e interpretado en conjunto, con el marco TIBER-EU y con los documentos que lo complementan —entre otros, la guía de contratación de proveedores *(TIBER-EU Services Procurement Guidelines)* y la guía del *White Team (TIBER-EU White Team Guidance)*— publicados por el BCE. Todas las referencias a documentos y plantillas publicados por el BCE incluidas en la presente guía pueden encontrarse en el sitio web de TIBER-EU[6].

Tanto las entidades financieras como los proveedores de servicios de *Threat Intelligence* (TI) o *Red Team* (RT) pueden dirigirse al TCT para formular cualquier duda respecto al presente documento o a los procesos en él descritos. Para ello, puede utilizarse el buzón de correo electrónico del equipo, tiberes@bde.es.

1.5 Introducción al proceso TIBER-ES

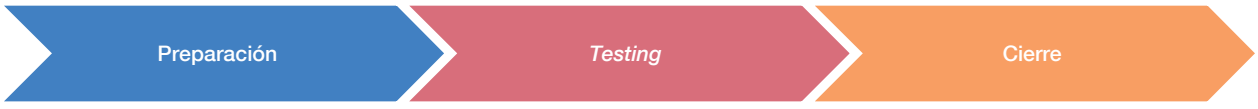
A continuación se describen, de forma breve, las principales fases de una prueba de *red teaming* bajo el esquema TIBER-ES, que sigue el modelo establecido en TIBER-EU. La descripción detallada del proceso se incluye en el epígrafe 3, «El proceso del test TIBER-ES».

El proceso de un test TIBER-ES se estructura en tres fases clave:

- **Fase de preparación:** se establecen los equipos responsables de la gestión integral del test y su alcance (focalizado en las funciones críticas de negocio), y se seleccionan los proveedores de TI y de RT que lo llevarán a cabo.

- **Fase de *testing:*** el proveedor de TI realizará un informe sobre la entidad que se somete al test, que se usará de base para la elaboración de escenarios de ataque. El proveedor de RT usará dichos escenarios de ataque en su aproximación a la entidad, con el objetivo de comprometer los sistemas informáticos en producción, los procesos o a las personas que forman parte del alcance de la prueba. El logro de dicho compromiso se atestiguará mediante la consecución de objetivos o la captura de banderas.

Esquema 1
PROCESO TIBER-ES



FUENTE: *TIBER Cyber Team.*

6 https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html.

— **Fase de cierre:** el proveedor de RT elaborará un informe de las actividades realizadas, que incluye detalles del proceso, recomendaciones de mejora y observaciones. Los equipos de seguridad defensiva de la entidad se involucrarán en esta fase del test y analizarán los resultados del RT; se podrán matizar o volver a ejecutar ciertas partes de los escenarios en una recreación de estos. La entidad elaborará un informe-resumen del test y desarrollará un plan de acción para la implementación de las recomendaciones de mejora acordadas.

1.6 ¿Quién puede someterse a este tipo de test?

Considerando el objetivo fundamental del marco TIBER-ES, fortalecer la ciberresiliencia de las entidades financieras que operan en España y contribuir a la estabilidad del sector financiero español, el marco es especialmente relevante para aquellas entidades más significativas o de carácter sistémico. En particular, los grandes bancos, aseguradoras y gestoras de activos, así como las infraestructuras críticas de mercado.

Además de dicho carácter sistémico, si bien cualquier entidad puede solicitar someterse a una prueba de *red teaming,* la sofisticación de estas pruebas las hace recomendables solo para las que ya tienen un cierto nivel de madurez en ciberresiliencia, ya que aquellas menos maduras posiblemente presenten debilidades que pueden detectarse mediante pruebas más sencillas y que conllevan un coste y un riesgo menores. El TCT tendrá en cuenta estas circunstancias para valorar la aceptación o denegación de las solicitudes de acceso a las pruebas. En cualquier caso, TIBER-ES pretende ser un catalizador eficaz para que todas las entidades mejoren sus capacidades de ciberseguridad hasta ser candidatas a someterse a este tipo de pruebas.

2 Participantes y funciones

2.1 El papel de las autoridades participantes

El Banco de España se constituye como autoridad propietaria de TIBER-ES. Por ello, es responsable del desarrollo y mantenimiento del marco operativo TIBER-ES, del que el presente documento forma parte. Estas funciones se realizan a través del TCT, en el que se integran el Banco de España, la CNMV y la DGSFP. La coordinación de las actuaciones del TCT recaerá sobre la autoridad a cuyo ámbito de competencia pertenezca la entidad objeto del test.

Por otra parte, se asignarán equipos en el ámbito del TCT, que monitorizarán la realización completa de las pruebas de *red teaming* bajo TIBER-ES, validarán que se llevan a cabo de acuerdo con los requisitos del marco y actuarán como garantes de los principios de TIBER-EU. En dichos equipos participarán, además del Banco de España, la CNMV y la DGSFP cuando las entidades objeto del test pertenezcan a sus respectivos ámbitos de competencia.

2.2 Participantes

2.2.1 *TIBER Cyber Team*

El Banco de España es el responsable de establecer la estructura de gobierno de TIBER-ES, que incluye la coordinación del TCT para la definición y gestión operativa de TIBER-ES.

Con carácter general, el TCT es responsable de las siguientes funciones, entre otras:

— Revisar periódicamente el marco TIBER-ES, aplicando las lecciones aprendidas de la implementación y los test realizados, y proponer las actualizaciones que procedan para su aprobación por el órgano competente del Banco de España.

— Participar en el *TIBER Knowledge Centre* (TKC) del BCE y proponer las correspondientes actualizaciones del marco TIBER-ES conforme a las decisiones tomadas en el TKC. Este es el foro común donde las autoridades de todas las jurisdicciones que han adoptado TIBER colaboran y cooperan en la implementación y actualización del marco TIBER-EU y sus guías.

— Invalidar los test si no se realizan de acuerdo con los requisitos de TIBER-ES y de TIBER-EU.

El TCT no desempeña un papel supervisor, y sus acciones no están ligadas a la imposición de requisitos en el caso de que se identifiquen debilidades durante la realización de los test. No es tampoco responsable de las acciones realizadas por la entidad que se somete al test o por sus proveedores, ni de los riesgos derivados de la prueba.

Por cada uno de los test de *red teaming* realizados bajo TIBER-ES, el TCT nombrará, entre sus integrantes, un *Team Test Manager* (TTM) con experiencia relevante en el sector, tanto en el campo

de la ciberresiliencia como en el de la gestión de proyectos. Su responsabilidad está limitada a la prueba en virtud de la cual se le ha nombrado, y debe:

— Realizar el seguimiento de la prueba, para asegurar que cumple con los requisitos de los marcos operativos TIBER-ES y TIBER-EU.

— Representar al TCT y coordinar sus acciones de apoyo al test a lo largo de todas sus fases, actuando como punto de contacto entre los distintos actores. Los puntos del proceso que requieren su intervención se concretan en el epígrafe 3, «El proceso del test TIBER-ES».

2.2.2 Entidad que se somete al test

White Team

Para cada test, la entidad que se somete a él ha de establecer un *White Team* (WT), que será el responsable último de la definición del alcance y de la ejecución efectiva del test. Asimismo, el WT tendrá la potestad de desistir de la ejecución de la prueba, siempre que concurran circunstancias objetivas que lo justifiquen. El número de miembros del WT deberá ser reducido, y estos guardarán la debida confidencialidad para no informar de la ejecución del test al resto de las divisiones y áreas de la entidad de la que forman parte. Su composición podrá variar en función de la fase y del desarrollo de las pruebas.

Este equipo será el encargado de gestionar los riesgos durante el test y estará formado por perfiles ejecutivos y de gestión de la entidad. Entre ellos deberá incluirse a expertos en ciberseguridad y a responsables de los procesos de escalado y notificación de ciberincidentes.

Se nombrará un *White Team Lead* (WTL) como responsable del WT dentro de la entidad, quien coordinará todas las actividades del test involucrando a todos los participantes, incluidos los proveedores.

Los requisitos sobre su composición, actividades y responsabilidades se recogen en la guía específica publicada por el BCE *(TIBER-EU White Team Guidance)*.

Blue Team

El *Blue Team* (BT) estará formado por todos los demás miembros de la entidad objeto del test, en particular por aquellos que gestionan el personal, los procesos y los sistemas que serán objeto de la prueba. El BT no deberá ser informado de la ejecución del test hasta que se llegue a la fase de cierre, cuando podrán participar en la recreación y en el seguimiento de las acciones correctoras que en su caso se decidan.

2.2.3 Proveedores

Antes de la ejecución de los test, la entidad debe acordar con los proveedores que participan al menos aspectos significativos como las condiciones económicas, el alcance previsto de las

pruebas, los límites en su ejecución y las actividades no permitidas, la duración del contrato, los recursos que empleará el proveedor, las acciones que se tomarán durante la ejecución del test y las responsabilidades que asumirán las partes, incluyendo la contratación de seguros si fuese necesario.

Es crucial que los proveedores y su personal cuenten con una adecuada independencia respecto de la entidad que se somete al test, de modo que se garantice la objetividad de los resultados, así como suficiente experiencia y habilidades acreditadas para la correcta y segura realización del test.

Un mismo proveedor podrá prestar simultáneamente las funciones de TI y de RT. No obstante, será deseable que ambas funciones sean asignadas a proveedores distintos cuando un único proveedor no pueda garantizar la suficiencia de recursos adecuados (tanto técnicos como humanos) en los equipos que desempeñan estos papeles.

Los requisitos en materia de independencia, experiencia y acuerdos con proveedores se recogen en la guía de contratación de proveedores publicada por el BCE *(TIBER-EU Services Procurement Guidelines)*.

Threat Intelligence

El proveedor de *Threat Intelligence* (TI) es un proveedor externo que ha de ser contratado por la entidad. Este proveedor recopilará información, replicando la investigación que realizaría un ciberatacante, y proveerá a la entidad que va a someterse al test de un informe de ciberinteligencia sobre amenazas específicas, que contendrá escenarios que podrían ser ejecutados por ciberatacantes reales. El proveedor deberá utilizar fuentes de información múltiples y actualizadas.

Red Team

El *Red Team* (RT) es un equipo proporcionado por un proveedor externo y contratado por la entidad. Tiene como objetivo comprometer las capacidades de seguridad de la entidad haciendo uso de TTP y métodos de *hacking* ético. Ejecutará sus ataques basándose en la información del proveedor de TI y en los escenarios que este haya diseñado. Al finalizar el test, elaborará un informe que detalle cómo se ejecutaron los escenarios y qué debilidades fueron encontradas.

3 El proceso del test TIBER-ES

A continuación se presenta una descripción detallada de las principales fases que conforman una prueba bajo el esquema TIBER-ES. Un test TIBER-ES consta de tres fases, siguiendo el modelo establecido en TIBER-EU. Cada una de estas fases se subdivide, a su vez, en diferentes pasos.

3.1 Fase de preparación

Esta fase comienza tras el acuerdo entre la entidad que se somete al test y el TCT para la realización de la prueba. Con ello, se da inicio al test TIBER-ES y el TCT empieza su colaboración con la entidad participante. Tiene una duración aproximada de cuatro-seis semanas, sin incluir el tiempo necesario para la contratación de los proveedores.

Se llevarán a cabo los siguientes pasos, siguiendo este orden:

1 Prelanzamiento:

— La entidad designará a un WTL y establecerá la composición del WT, que el TTM deberá validar. Para ello, y como referencia, tanto la entidad como el TTM utilizarán la guía específica publicada por el BCE *(TIBER-EU White Team Guidance)*. El WT será el responsable de la gestión integral del test (su papel se describe en detalle en el epígrafe 2, «Participantes y funciones», así como en la mencionada guía específica del BCE).

— Se celebrará una reunión de prelanzamiento, en la que el TTM explicará al WT el proceso del test y sus características, según están reflejadas en la presente guía de implementación de TIBER-ES. Se tratarán los requisitos respecto a las partes involucradas y sus responsabilidades, los protocolos de seguridad y de confidencialidad que se utilizarán (incluyendo los de envío e intercambio de documentación entre los participantes) y la planificación preliminar de la prueba.

— El WT adoptará las medidas necesarias para la gestión de los riesgos derivados del test, con el objetivo de garantizar su realización de una manera controlada y acorde con el apetito al riesgo de la entidad (véase el epígrafe 4, «Gestión de riesgos»).

Esquema 2
FASE DE PREPARACIÓN

FUENTE: *TIBER Cyber Team.*

2 Contratación de proveedores:

— El WT dará inicio al proceso de identificación de potenciales proveedores de TI y de RT. Aunque la entidad ya esté llevando a cabo pruebas de *red teaming* utilizando sus propios equipos de TI y/o de RT internos, el TCT solo validará la prueba bajo el esquema TIBER-ES si esta se lleva a cabo por proveedores externos que cuenten con una adecuada independencia respecto a la entidad y a su BT, con el objetivo de garantizar la objetividad de los resultados y la debida discreción durante la realización del test. Los referidos proveedores externos deberán acreditar suficiente experiencia previa en este tipo de pruebas, así como habilidades y conocimientos técnicos para la correcta y segura realización de los test.

  Durante este proceso, el WT deberá observar los requisitos y principios contenidos en la guía de contratación de proveedores publicada por el BCE *(TIBER-EU Services Procurement Guidelines).*

— La entidad iniciará el proceso de contratación, evaluará las propuestas de los distintos proveedores y procederá a la adjudicación de los servicios.

— Se formalizarán los contratos entre las partes (entidad y proveedores), que incluirán, entre otros, aspectos como las condiciones económicas, el alcance previsto de las pruebas, los límites en su ejecución y las actividades no permitidas, la duración del contrato, los recursos que empleará el proveedor, las acciones que se tomarán durante la ejecución del test y las responsabilidades que asumirán las partes, incluyendo la contratación de seguros si fuese necesario. Asimismo, se regularán la no divulgación y la confidencialidad, los requisitos de destrucción de datos, así como la notificación temprana al cliente de posibles vulnerabilidades críticas que se detecten durante la realización de las pruebas.

  Dado que es habitual que la formalización de los contratos requiera un período de negociación prolongado, podrá continuarse, en paralelo a dicha negociación, con el resto de los pasos que componen la fase, siempre que se hayan formalizado los correspondientes acuerdos de confidencialidad entre las partes.

3 Lanzamiento:

— Una vez seleccionados los proveedores de TI y de RT, el WT completará la planificación de las pruebas y la agenda de reuniones con los participantes.

— El WT celebrará una reunión de lanzamiento del proceso, con la participación de miembros del TCT, así como de los proveedores de TI y de RT. En ella se detallarán el proceso del test y las expectativas de la entidad, su planificación y un cronograma que incluya las reuniones y los puntos de control básicos, así como los documentos y entregables esperados en cada fase planificada.

4 Definición del alcance:

— El WT definirá el alcance preliminar de la prueba, que deberá incluir funciones críticas de la entidad[7] y los sistemas y servicios que soportan dichas funciones. Opcionalmente, el WT podrá incluir también funciones no críticas. Para definir cuáles son sus funciones críticas, las entidades deberán apoyarse en análisis internos, como los análisis de impacto de negocio *[Business Impact Analysis* (BIA)].

Existe la posibilidad de que estas funciones críticas estén total o parcialmente externalizadas. En caso de que así fuera, la entidad valorará la viabilidad de incluir a un representante del proveedor en quien se externalice total o parcialmente la función crítica como miembro del WT. El objetivo será, en último término, poder desarrollar la prueba sobre la función externalizada con los mismos requisitos y de la misma manera que si no existiera dicha externalización.

Sobre los sistemas y servicios que dan soporte a las funciones críticas de negocio, el WT establecerá los objetivos o las banderas a capturar por el RT durante la prueba. No obstante, estos objetivos podrán ser actualizados a medida que el proveedor de TI obtenga ciberinteligencia adicional y el RT ejecute el test. Si bien la prueba ha de realizarse sobre sistemas en entornos de producción de la entidad, estos objetivos podrán incluir adicionalmente sistemas en entornos de preproducción, de test o de recuperación de desastres.

Para la elaboración del documento de alcance preliminar, se recomienda la utilización de la plantilla de definición de alcance publicada por el BCE *(TIBER-EU Scope Specification Template)*.

— El WT compartirá con el TCT y con los proveedores de TI y de RT el documento de alcance preliminar, con el fin de incorporar sus aportaciones. Para ello, el TCT deberá tener un amplio conocimiento del modelo de negocio de la entidad, así como de sus funciones críticas y servicios. Adicionalmente, el TCT podrá consultar a la autoridad supervisora o de vigilancia de la entidad, ya sea esta de ámbito nacional o supranacional (como, por ejemplo, los *Joint Supervisory Teams* del BCE).

— El WT celebrará una reunión de definición de alcance para exponer el documento de alcance preliminar y obtendrá la validación del TCT y de los proveedores de TI y de RT.

— El WT recabará la aprobación formal y la firma del documento de alcance preliminar del consejo de administración de la entidad. Con el documento de alcance aprobado, si fuera preciso, se modificará la planificación.

7 Las funciones críticas de la entidad, según el test TIBER-ES, se definen como las personas, los procesos y las tecnologías requeridos por la entidad para prestar servicios críticos, los cuales, si fuesen interrumpidos, tendrían un impacto perjudicial en la estabilidad financiera, la seguridad y la solidez de la entidad, sus clientes o la conducta de la entidad en el mercado. No se trata de un sistema, sino de una función de negocio esencial para el sector o para la entidad.

Cuadro 1

FASE DE PREPARACIÓN

Objetivo	Entregable o hito	Responsable	Validación
Establecimiento del WT	– WT establecido	Entidad	TTM
Prelanzamiento	– Reunión de prelanzamiento – Planificación preliminar de las pruebas	WT	
Gestión de riesgos	– Análisis preliminar de riesgos – Definición de medidas de mitigación/transferencia	WT	
Contratación de proveedores de TI y de RT	– Licitación, evaluación de propuestas y adjudicación de servicios – Cláusulas de confidencialidad con proveedores de TI y de RT – Contratos con proveedores de TI y de RT seleccionados – Contratación de ciberseguro (opcional)	WT	
Lanzamiento	– Planificación de las pruebas – Reunión de lanzamiento – Cronograma del proceso – Puntos de control y entregables	WT	
Definición del alcance y de los objetivos	– Reunión de definición de alcance – Documento de alcance preliminar	WT	TCT Prov. TI/RT
	– Documento de alcance	WT	Consejo

FUENTE: *TIBER Cyber Team.*

3.2 Fase de test

Esta fase engloba la recopilación de información y la elaboración de un informe de ciberinteligencia por parte del proveedor de TI, así como la definición del plan de test y su ejecución por parte del RT. Tiene una duración aproximada de 16-18 semanas.

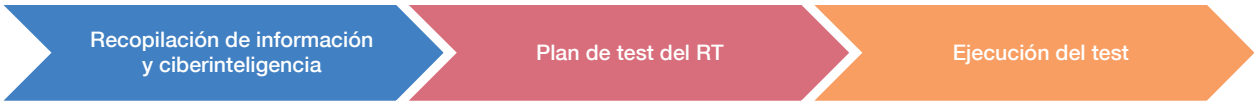
Se llevarán a cabo los siguientes pasos, siguiendo este orden:

1 Recopilación de información y ciberinteligencia:

En esta actividad se pretende emular la tarea de recopilación de información previa a un ataque, que un ciberatacante real desarrollaría como fase de reconocimiento. Es necesario que la información recopilada sea relevante para el alcance del test, establecido en la fase previa (véase el epígrafe 3.1, «Fase de preparación»). La información recopilada se usa de base para la elaboración de escenarios de ataque, específicamente diseñados para que resulten factibles y significativos, y tengan un impacto relevante para la entidad objetivo. En este primer paso de ciberinteligencia es importante reflejar las amenazas más importantes a las que se enfrenta, así como conseguir una visión lo más detallada posible de los mecanismos de defensa y de la superficie de exposición de la entidad. De esta forma se pueden emplear o imitar las TTP que un ciberatacante real utilizaría. La duración estimada de este paso es de cinco semanas.

Existen dos herramientas de ciberinteligencia, complementarias entre sí, para desarrollar los escenarios basados en amenazas: el informe de amenazas genéricas *[Generic Threat Landscape* (GTL)], para el sector en el que opera la entidad, y el informe específico de amenazas concernientes a la entidad que participa en el test TIBER-ES *[Targeted Threat Intelligence* (TTI)].

Esquema 3
FASE DE TEST



FUENTE: *TIBER Cyber Team.*

El informe GTL para el sector financiero es un informe elaborado habitualmente por proveedores especializados o por autoridades de ciberseguridad y/o de ciberinteligencia nacionales. En caso de existir, se recomendará usarlo como base para la elaboración del TTI.

Atendiendo a lo anterior:

— El TCT facilitará al proveedor de TI de la entidad el informe GTL, en caso de disponer de dicho informe.

— El proveedor de TI elaborará el informe TTI. Podrá ayudarse de la guía para la elaboración de este tipo de informes publicada por el BCE *(TIBER-EU Guidance for Target Threat Intelligence Report)*. Para añadir el mayor valor posible al test, se recomienda encarecidamente que la entidad facilite al proveedor de TI información relevante sobre las amenazas y las vulnerabilidades que podría utilizar un ciberatacante real. La naturaleza de la información a aportar por la entidad debería ser comparable a la que habría podido obtener un ciberatacante que dispusiese de tiempo ilimitado y no tuviera restricciones morales, éticas o legales. El proveedor de TI también recopilará por sus propios medios información adicional de la entidad, bien sea pública, bien haya sido filtrada involuntariamente.

  El TTI contendrá datos relativos a los sistemas que soportan las funciones críticas, el registro de amenazas a las que podría exponerse la entidad, los actores que podrían llevar a cabo ciberataques, ejemplos de ataques recientes y, finalmente, los probables escenarios de ataque. Dichos escenarios han de ser realistas y útiles para el futuro plan de test que realizará el RT, y deben incluir las motivaciones de los ciberatacantes y los objetivos que pretenden lograr.

— El proveedor de TI facilitará el borrador del informe TTI al WT, al RT y al TCT para su revisión.

— El WT celebrará una reunión específica para validar el TTI. Es particularmente relevante la validación por parte del RT de los escenarios de ataque definidos, dado que deberá elaborar un plan de test con estos. No obstante, el informe TTI podrá ser actualizado durante la elaboración del plan de test del RT, e incluso durante la ejecución de las pruebas, si es necesario y así lo acuerdan los participantes.

2 Plan de test del RT:

La duración estimada de este paso es de una-dos semanas.

— El RT elaborará un plan de test con base en el informe TTI. Para ello, podrá ayudarse de la guía para el plan de test del RT publicada por el BCE *(TIBER-EU Guidance for the Red Team Test Plan)*. Los objetivos del test, que fueron acordados durante el paso de definición del alcance y posiblemente actualizados durante la elaboración del informe TTI, serán las banderas a capturar por el RT durante la ejecución.

  Opcionalmente, la entidad podrá proveer al RT de información relevante para simular mejor las condiciones de un ataque real. El WT tomará las medidas necesarias para asistir al RT si así lo solicita el proveedor.

  El plan de test del RT estará formado por una serie de escenarios que representarán objetivos concretos a lograr. Para su definición, el RT se basará en los escenarios definidos en el informe TTI, si bien podrá incluir nuevos escenarios que se estimen relevantes, o una combinación de escenarios ya presentes. El RT deberá utilizar su conocimiento y experiencia, combinando la ciberinteligencia interna disponible con la información obtenida de fuentes abiertas, para definir alternativas dentro de los escenarios base u originales en caso de que no funcione la primera opción de ataque.

— Una vez finalizados el informe TTI y el plan de test del RT, el WT convocará una reunión para que los proveedores de TI y de RT discutan los detalles operacionales, y en la que participará el TCT.

3 Ejecución del test:

El tiempo asignado a la tarea del RT debe estar alineado con el alcance definido, así como con la capacidad y los recursos del WT y del RT. Un tiempo de referencia para la ejecución del test del RT es de 10-12 semanas.

A partir de este momento, el RT es el que toma el mando de la ejecución del test. El RT deberá desarrollar técnicas alternativas de ataque en caso de encontrar obstáculos para lograr los objetivos o capturar las banderas asignadas.

En ocasiones, el RT puede requerir al WT asistencia para deshabilitar barreras internas y/o controles de seguridad de la entidad, con el fin de facilitar el progreso del test. Un ejemplo sería permitir el acceso a un sistema o segmento de la red interna para poder continuar con el test y progresar hacia el siguiente objetivo o bandera. Esta situación se puede dar cuando el BT de la entidad logra defender dicho objetivo o bandera de manera efectiva, o en el caso de procesos que tanto el WT como el RT determinan como triviales y en cuyo desarrollo un ciberatacante externo tendría éxito si empleara el tiempo necesario. Si el RT hiciese una petición de este tipo y esta fuera concedida, deberá reflejarse en los informes, puesto que los resultados que puedan producirse a partir de la desconexión de un control o mecanismo de seguridad deben ser puestos en un contexto propio.

Cuadro 2

FASE DE TEST

Objetivo	Entregable o hito	Responsable	Validación
Inteligencia genérica	– Entrega al proveedor de TI del informe de int. genérica (opcional)	TCT	
Inteligencia específica	– Contribución de la entidad al desarrollo del informe TTI mediante información relevante sobre amenazas y vulnerabilidades que podría utilizar un atacante real (opcional)	WT	
	– Informe TTI preliminar	Prov. TI	
	– Reunión de validación del informe TTI – Informe TTI	WT Prov. TI	WT/TCT/RT
Definición del plan de test y de los escenarios	– Contribución de la entidad al desarrollo del plan de test y a la definición de escenarios realistas y significativos por parte del proveedor de RT mediante información que podría utilizar un atacante real (opcional)	WT	
	– Plan de test del RT	RT	
Coordinación previa a la ejecución	– Reunión de coordinación entre los proveedores de TI y de RT	WT	
Ejecución del plan de test del RT	– Registro de acciones ejecutadas	RT	
	– Deshabilitar barreras internas y/o controles de seguridad de la entidad con el fin de facilitar el progreso del test (opcional)	WT/RT	
Información constante sobre el avance	– Informes periódicos (al menos semanales) al WT y al TCT sobre el grado de avance del test	RT	
Coordinación durante la ejecución	– Reuniones periódicas de seguimiento y coordinación del test entre el proveedor de RT, el TCT y el WT. Podrá incluirse, cuando se considere necesario, al proveedor de TI (opcional)	WT	

FUENTE: *TIBER Cyber Team.*

El RT mantendrá continuamente informado al WT de los progresos, y deberá informar al menos semanalmente al TCT del avance de la ejecución del test. Si es posible, se recomienda mantener reuniones durante este paso entre el RT, el WT y el TCT, e incluir al proveedor de TI si se considerara necesario, ya que añade un valor significativo a la calidad del test y ayuda a la confianza entre las partes. Es crucial que el BT no esté al tanto de estas reuniones.

Todas las acciones del RT habrán de ser registradas para que, tras la fase de test, el BT pueda reproducirlas.

3.3 Fase de cierre

La fase de cierre permite a todas las partes implicadas reflejar los resultados del test y señalar las mejoras que necesita la entidad para fortalecer su ciberresiliencia. En ella se elaboran los informes del test, en los que se señalarán aspectos de mejora relacionados con controles técnicos, políticas, procedimientos y procesos, así como con concienciación y formación del personal. Se recrea y se comenta el plan ejecutado con el BT, se define un plan de acción para la implementación de las recomendaciones de mejora, se comparten los resultados con las partes implicadas y se valida, mediante la firma de un documento específico al efecto, la idoneidad de la ejecución del test respecto al marco TIBER-ES. La duración estimada para esta fase es de cuatro semanas.

Esquema 4
FASE DE CIERRE

FUENTE: *TIBER Cyber Team.*

Se llevarán a cabo los siguientes pasos, siguiendo este orden:

1 **Elaboración de informes del RT y del BT:**

— El RT enviará al WT y al TCT su borrador del informe del test *[Red Team Test Report* (RTTR)] en un plazo máximo de dos semanas después de finalizar el test. Para elaborarlo, se ayudará preferiblemente de la guía para el informe del test del RT publicada por el BCE *(TIBER-EU Guidance for the Red Team Test Report).*

— El WT informará del test efectuado a los miembros clave del BT de la entidad, quienes utilizarán el RTTR para elaborar su propio informe. Ese informe del BT *[Blue Team Test Report* (BTTR)] relacionará sus acciones con las acciones del RT y será completado antes de recrear el test del RT (véase el siguiente apartado) para obtener el máximo provecho de las lecciones aprendidas.

2 **Recreación del test, lecciones aprendidas y plan de acción:**

— El test será recreado por el RT y el BT, y ambas partes revisarán los pasos dados. Para ello, el RT podrá utilizar los registros de las acciones realizadas. No será estrictamente necesaria la recreación completa ni en entornos de producción.

El fin es aprender de la experiencia proporcionada por la ejecución del test, en colaboración con el proveedor de RT. Adicionalmente, el RT deberá dar su opinión sobre qué objetivos podría haber logrado un ciberatacante real, con más tiempo y medios que los empleados en un test TIBER-ES.

— Opcionalmente, se puede crear un *Purple Team,* compuesto por miembros del RT y del BT, con el objetivo de trabajar conjuntamente en analizar qué opciones podría haber tomado el RT en el test y cómo podría haber respondido el BT ante ellos.

— Posteriormente, el WT llevará a cabo una reunión de evaluación entre todas las partes que intervienen en el test: la entidad (representada por el WT), el TCT y los proveedores

de TI y de RT. En esta reunión se evaluarán las lecciones aprendidas en la ejecución de la prueba, que servirán para futuros test. Adicionalmente, se recabarán opiniones sobre otros aspectos de relevancia para la mejora del marco TIBER-ES y de la presente guía.

— La entidad deberá elaborar un plan de acción para la implementación de las recomendaciones de mejora acordadas. Este plan, que deberá ser acordado con los proveedores de TI y de RT, así como con el TCT, servirá para realizar mejoras que permitan mitigar o solventar las debilidades encontradas durante el test y mejorar la ciberresiliencia de la entidad.

— La entidad enviará el plan de acción para la implementación de las recomendaciones de mejora a su autoridad supervisora o de vigilancia, ya sea esta de ámbito nacional o supranacional.

3 **Informe-resumen del test:**

— La entidad elaborará un informe-resumen del test basándose en documentos como el informe TTI, el plan de test del RT, los informes RTTR y BTTR, y el plan de acción para la implementación de las recomendaciones de mejora. Para elaborarlo, se ayudará preferiblemente de la guía para el informe-resumen del test publicada por el BCE *(Guidance for the TIBER-EU Test Summary Report).* Este informe no contendrá información técnica detallada de las debilidades y vulnerabilidades encontradas, dado que esa información está destinada solo a la entidad, debido a su elevada confidencialidad. El informe será compartido con el TCT, que podrá revisar las conclusiones del test de manera más detallada si lo considera necesario.

— La entidad enviará el informe-resumen a su autoridad supervisora o de vigilancia, ya sea esta de ámbito nacional o supranacional.

4 **Validación del test:**

Al finalizar el test, y cuando se haya acordado el plan de acción para la implementación de las recomendaciones de mejora, el WT, los proveedores de TI y de RT, y el TCT deben validar que el test se ha realizado de acuerdo con los requisitos del marco TIBER-ES. El WT dará fe de ello en un documento que debe estar firmado por el consejo de administración de la entidad y por los proveedores, y que permitirá, siempre que esté validado por el TCT, el reconocimiento mutuo ante autoridades de otras jurisdicciones que hayan adoptado localmente el marco TIBER-EU. Como soporte documental, se utilizará como referencia la plantilla de validación publicada por el BCE *(TIBER-EU Attestation Template).*

Cuadro 3

FASE DE CIERRE

Objetivo	Entregable o hito	Responsable	Validación
Conclusiones del RT	– RTTR enviado al WT y al TCT	RT	
Comunicación al BT del test efectuado	– El WT informará a los miembros clave del BT de la entidad sobre el test efectuado	WT	
Conclusiones del BT	– BTTR enviado al WT y al TCT	BT	
Recreación del test	– El test será recreado de acuerdo con el criterio del RT y del BT, y ambas partes revisarán los pasos dados	RT/BT	
Aprovechamiento de lecciones aprendidas	– Creación del *Purple Team* a partir del RT y del BT (opcional)	WT	
Evaluación del proceso	– Reunión de evaluación y *feedback* de todos los actores implicados en el proceso: WT, BT, TCT y proveedores de TI y de RT	WT	
Plan de acción	– Plan de acción para la implementación de las recomendaciones de mejora	WT	TCT Prov. TI/RT
	– Envío a la autoridad supervisora del plan de acción para la implementación de las recomendaciones de mejora	WT	
Validación del test	– Validación y firma formal del cumplimiento de los requisitos del marco TIBER-ES	WT Prov. TI/RT Consejo	TCT

FUENTE: *TIBER Cyber Team.*

4 Gestión de riesgos

La gestión de los riesgos en los test realizados bajo el esquema TIBER-ES es un punto fundamental, dado el requisito de realizar test de ciberresiliencia flexibles y realistas sobre entornos de producción. Esto implica riesgos con respecto a la confidencialidad, integridad y disponibilidad de los sistemas y de los datos (incluidos datos particularmente sensibles y protegidos por la regulación vigente, como los de carácter personal). Una inadecuada ejecución de los test podría causar daños o fallos en los sistemas y aplicaciones, así como modificaciones, borrados o filtraciones ilícitas de datos.

Es clave realizar, en primer lugar, una identificación y un análisis detallado de los riesgos que podrían materializarse al ejecutar el test y tomar acciones apropiadas para mitigarlos antes, durante y después de este. Para ello, es fundamental disponer de un plan de contingencias. El WT es el responsable de asegurar que los riesgos asociados a la realización de los test bajo el esquema TIBER-ES son identificados, analizados y mitigados en todo momento. El TCT monitorizará la ejecución de los test, pero no será responsable de ningún daño causado a las entidades en su ejecución. Asimismo, la contratación de ciberseguros es una alternativa para complementar la mitigación del riesgo con estrategias de transferencia.

Por todo ello, es importante que los proveedores de TI y de RT elegidos cumplan los requisitos mínimos establecidos en las *TIBER-EU Services Procurement Guidelines.* Los contratos con los proveedores deberán incluir cláusulas de confidencialidad y cubrir aspectos como los requisitos de seguridad, las responsabilidades, las indemnizaciones, los límites en la ejecución y las actividades que no están permitidas durante la realización del test. Ejemplos de actividades no permitidas podrían ser la destrucción de equipos o de datos, la modificación descontrolada de datos o de programas, el comprometer la continuidad de sistemas críticos, las extorsiones o amenazas a empleados, o la publicación de los resultados del test.

Respecto a la confidencialidad en la realización de las pruebas, se debe asegurar que nadie en la entidad, salvo el WT, esté al tanto del test, y para ello podrán firmarse acuerdos de confidencialidad *(non-disclosure agreements)* con los proveedores[8]. Los participantes en el test deberán usar nombres codificados para la entidad con el fin de proteger su identidad. El WT deberá gestionar el escalado de los ciberincidentes relacionados con el test para que no se ejecuten acciones que se llevarían a cabo de manera obligatoria en caso de ocurrir un ciberincidente real, como comunicarse con terceros, entre ellos las Fuerzas y Cuerpos de Seguridad del Estado. Si el TTM sospecha de que el BT está al tanto del test y de que trata de manipular sus resultados, podrá no validar que la prueba se ha realizado de acuerdo con los requisitos del marco TIBER-ES.

8 En el caso de las autoridades, las informaciones o los datos de carácter reservado que las entidades faciliten están sujetos al deber de secreto profesional en el marco de la legislación vigente.

5 Los resultados y su uso en la supervisión financiera y en la vigilancia

Los detalles del resultado de un test realizado bajo el esquema TIBER-ES son única y exclusivamente propiedad de la entidad que se somete a él. Por razones de seguridad, el carácter altamente confidencial de la información contenida en informes como el RTTR o el BTTR hace desaconsejable compartirlos con terceros. Esta recomendación es de aplicación a los proveedores de RT y de TI, así como al TCT, que no deberán almacenar o mantener información confidencial de la entidad más allá del período de tiempo necesario para la realización de la prueba.

El plan de acción para la implementación de las recomendaciones de mejora y el informe-resumen del test constituyen una excepción a lo anteriormente estipulado, dado que serán elaborados abstrayendo los detalles técnicos y con el fin de ser compartidos con la autoridad supervisora o de vigilancia y con el TCT, así como con quienes la entidad considere oportuno. Pueden encontrarse más detalles al respecto en el epígrafe 3, «El proceso del test TIBER-ES».

Adicionalmente, el TCT puede compartir con el TKC información extraída del plan de acción para la implementación de las recomendaciones de mejora o del informe-resumen del test, como, por ejemplo, vulnerabilidades encontradas o lecciones aprendidas. Dicha información se anonimizará y se intercambiará usando siempre canales seguros. El objetivo es permitir al TKC agregar datos sobre aspectos clave y comunes con el fin de conformar una imagen del estado de la ciberresiliencia del sector financiero europeo.

Como se especifica en el epígrafe 1, «Introducción», el marco TIBER-ES se adopta desde una perspectiva de estabilidad financiera. Por ello, el equipo encargado de la supervisión o de la vigilancia ordinaria de la entidad tendrá una implicación limitada en el test y estará involucrado en unas fases del proceso muy específicas:

— Fase de preparación: la entidad comunicará, a título informativo, el comienzo de la realización del test TIBER-ES al equipo encargado de la supervisión o de la vigilancia ordinaria de la entidad. Asimismo, el TCT podrá consultar a la autoridad supervisora o de vigilancia si el alcance definido por el WT para la prueba cubre funciones críticas de la entidad.

— Fase de cierre: la entidad enviará a su autoridad supervisora o de vigilancia el informe-resumen del test y el plan de acción para la implementación de las recomendaciones de mejora.

Anejo Matriz de responsabilidades

Cuadro A.1

FASE DE PREPARACIÓN

Objetivo	Entregable o hito	Responsable	Validación
Establecimiento del WT	– WT establecido	Entidad	TTM
Prelanzamiento	– Reunión de prelanzamiento – Planificación preliminar de las pruebas	WT	
Gestión de riesgos	– Análisis preliminar de riesgos – Definición de medidas de mitigación/transferencia	WT	
Contratación de proveedores de TI y de RT	– Licitación, evaluación de propuestas y adjudicación de servicios – Cláusulas de confidencialidad con proveedores de TI y de RT – Contratos con proveedores de TI y de RT seleccionados – Contratación de ciberseguro (opcional)	WT	
Lanzamiento	– Planificación de las pruebas – Reunión de lanzamiento – Cronograma del proceso – Puntos de control y entregables	WT	
Definición del alcance y de los objetivos	– Reunión de definición de alcance – Documento de alcance preliminar	WT	TCT Prov. TI/RT
	– Documento de alcance	WT	Consejo

FUENTE: *TIBER Cyber Team.*

Cuadro A.2

FASE DE TEST

Objetivo	Entregable o hito	Responsable	Validación
Inteligencia genérica	– Entrega al proveedor de TI del informe de int. genérica (opcional)	TCT	
Inteligencia específica	– Contribución de la entidad al desarrollo del informe TTI mediante información relevante sobre amenazas y vulnerabilidades que podría utilizar un atacante real (opcional)	WT	
	– Informe TTI preliminar	Prov. TI	
	– Reunión de validación del informe TTI – Informe TTI	WT Prov. TI	WT/TCT/RT
Definición del plan de test y de los escenarios	– Contribución de la entidad al desarrollo del plan de test y a la definición de escenarios realistas y significativos por parte del proveedor de RT mediante información que podría utilizar un atacante real (opcional)	WT	
	– Plan de test del RT	RT	
Coordinación previa a la ejecución	– Reunión de coordinación entre los proveedores de TI y de RT	WT	
Ejecución del plan de test del RT	– Registro de acciones ejecutadas	RT	
	– Deshabilitar barreras internas y/o controles de seguridad de la entidad con el fin de facilitar el progreso del test (opcional)	WT/RT	
Información constante sobre el avance	– Informes periódicos (al menos semanales) al WT y al TCT sobre el grado de avance del test	RT	
Coordinación durante la ejecución	– Reuniones periódicas de seguimiento y coordinación del test entre el proveedor de RT, el TCT y el WT. Podrá incluirse, cuando se considere necesario, al proveedor de TI (opcional)	WT	

FUENTE: *TIBER Cyber Team.*

Cuadro A.3

FASE DE CIERRE

Objetivo	Entregable o hito	Responsable	Validación
Conclusiones del RT	– RTTR enviado al WT y al TCT	RT	
Comunicación al BT del test efectuado	– El WT informará a los miembros clave del BT de la entidad sobre el test efectuado	WT	
Conclusiones del BT	– BTTR enviado al WT y al TCT	BT	
Recreación del test	– El test será recreado de acuerdo con el criterio del RT y del BT, y ambas partes revisarán los pasos dados	RT/BT	
Aprovechamiento de lecciones aprendidas	– Creación del *Purple Team* a partir del RT y del BT (opcional)	WT	
Evaluación del proceso	– Reunión de evaluación y *feedback* de todos los actores implicados en el proceso: WT, BT, TCT y proveedores de TI y de RT	WT	
Plan de acción	– Plan de acción para la implementación de las recomendaciones de mejora	WT	TCT Prov. TI/RT
	– Envío a la autoridad supervisora del plan de acción para la implementación de las recomendaciones de mejora	WT	
Validación del test	– Validación y firma formal del cumplimiento de los requisitos del marco TIBER-ES	WT Prov. TI/RT Consejo	TCT

FUENTE: *TIBER Cyber Team.*

BANCO DE ESPAÑA
Eurosistema

GOBIERNO DE ESPAÑA

VICEPRESIDENCIA PRIMERA DEL GOBIERNO

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO DE ECONOMÍA Y APOYO A LA EMPRESA

DIRECCIÓN GENERAL DE SEGUROS Y FONDOS DE PENSIONES

CNMV
Comisión Nacional del Mercado de Valores